MINISTERIO DE CIENCIA, INNOVACIÓN, TECNOLOGÍA Y TELECOMUNICACIONES

GOBIERNO DE COSTA RICA

Informe sobre Construcción de la Estrategia Nacional de Ciberseguridad 2023-2027

CSIRT-CR

2023

Contenido

Presentación o Introducción

El presente es un informe sobre la construcción de la Estrategia Nacional de Ciberseguridad en el cual el Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones de Costa Rica (MICITT) con el apoyo del Programa de Ciberseguridad del Comité Interamericano contra el Terrorismo (CICTE) de la Organización de Estados Americanos (OEA) viene adelantando un proceso participativo de formulación de la nueva Estrategia Nacional de Ciberseguridad de Costa Rica 2023-2027 en donde se articule una visión estratégica bajo un modelo institucional eficiente robusteciendo el liderazgo del Gobierno nacional y se vincule a todas las partes interesadas bajo un enfoque de derechos humanos y en línea con la construcción de una sociedad incluyente en todos los ámbitos de la vida costarricense.

Análisis o Hallazgos

El Gobierno de Costa Rica con el liderazgo del Ministerio de Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones de Costa Rica (MICITT) y con el apoyo del Programa de Ciberseguridad del Comité Interamericano contra el Terrorismo (CICTE) de la Organización de Estados Americanos (OEA) viene adelantando un proceso participativo de formulación de una nueva Estrategia Nacional de Ciberseguridad 2023-2027 en donde se articule una visión estratégica bajo un modelo institucional eficiente robusteciendo el liderazgo del Gobierno nacional y se vincule a todas las partes interesadas bajo un enfoque de derechos humanos y en línea con la construcción de una sociedad incluyente en todos los ámbitos de la vida costarricense.

Bajo este proceso, durante los días 11, 12, 13 y 14 de septiembre de 2023, el MICITT llevó a cabo 4 mesas virtuales con el apoyo del Programa de Ciberseguridad del CICTE de la OEA con un total de 190 participantes (69% hombres y 31% mujeres). En estas mesas virtuales con las múltiples partes interesadas del ecosistema de ciberseguridad de Costa Rica se discutió la nueva propuesta de Estrategia Nacional de Ciberseguridad 2023–2027 dadas las actuales condiciones del país. En estos espacios, los participantes presentaron i) sus consideraciones acerca de la nueva propuesta, y ii) sus recomendaciones de acciones de corto, mediano o largo plazo urgentes y/o necesarias con el fin de mejorar la gestión de ciberseguridad en el país mediante el diligenciamiento de un formulario electrónico.

Adicionalmente, durante los días 20 y 21 de septiembre de 2023, el MICITT y el Programa de Ciberseguridad del CICTE de la OEA lideraron el desarrollo de mesas técnicas presenciales que tuvieron la posibilidad de tener asistentes virtuales. En este encuentro presencial participaron 137 personas representando a 97 organizaciones (públicas y privadas) de las cuales: i) 74 estuvieron de manera presencial (54%) y 63 de manera virtual (46%) y ii) 90 fueron hombres (66%) y 47 fueron mujeres (34%).

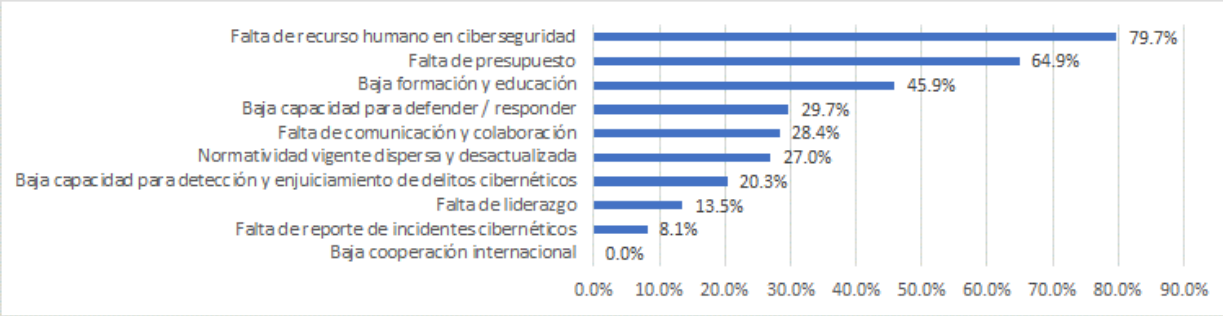
En estas mesas presenciales, la OEA compartió las tendencias globales de ciberseguridad, el estado regional en torno a la formulación de estrategias nacionales de ciberseguridad, algunos casos de éxito en y mejores prácticas internacionales en torno a la formulación. Por su parte, el MICITT presentó una propuesta de nueva Estrategia Nacional de Ciberseguridad y una propuesta de Plan de Acción. Adicionalmente se dispusieron 6 encuestas que se diligenciaron en vivo logrando obtener insumos valiosos para el proceso.

El presente documento presenta los resultados de las mesas de trabajo virtuales y presenciales para la formulación de la Estrategia Nacional de Ciberseguridad 2023-2027 de Costa Rica, basado en las mejores prácticas internacionales y regionales, teniendo en cuenta la implementación de la Estrategia Nacional de Ciberseguridad 2017, y examinado a través de las evaluaciones existentes recibidas del Gobierno nacional. Se analizaron los desafíos / retos actuales, la visión, los principios, el propósito general, los objetivos específicos y las acciones estratégicas.

A continuación, se presentan los aportes en relación con la validación del marco estratégico de la nueva estrategia y en relación con la importancia de las acciones propuestas en el Plan de Acción que acompaña la nueva estrategia.

PRINCIPALES RETOS EN EL PAÍS

¿Cuáles son los principales problemas del país en torno a la ciberseguridad? Escoja los 3 problemas más relevantes.

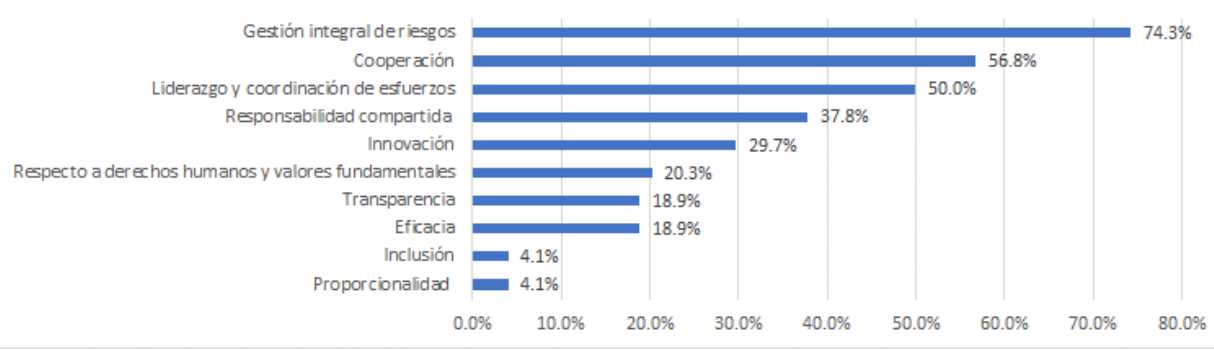


Nota: 74 respuestas

RELEVANCIA DE PRINCIPIOS ORIENTADORES

¿Cuáles serían los principios orientadores de la nueva estrategia de ciberseguridad para el país?

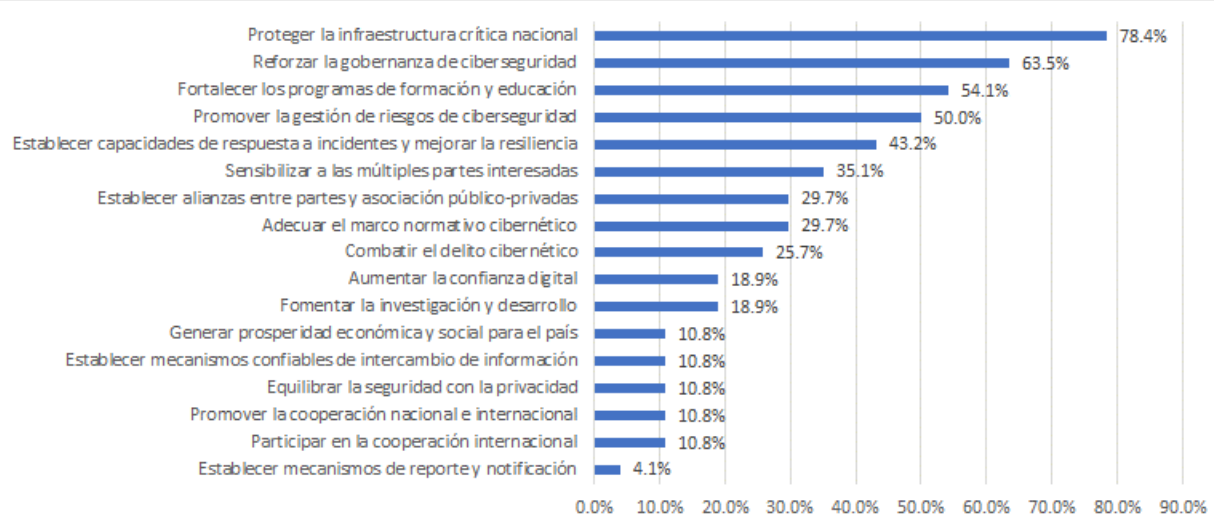
Escoja los 3 principios más relevantes.



Nota: 74 respuestas

PRIORIZACIÓN DE OBJETIVOS

¿Cuáles serían los objetivos de la nueva estrategia de ciberseguridad en el país? Escoja los 5 objetivos más relevantes.



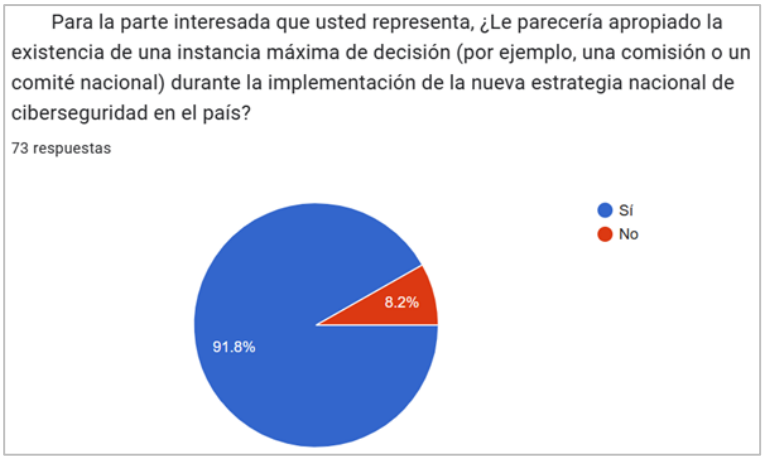
Nota: 74 respuestas

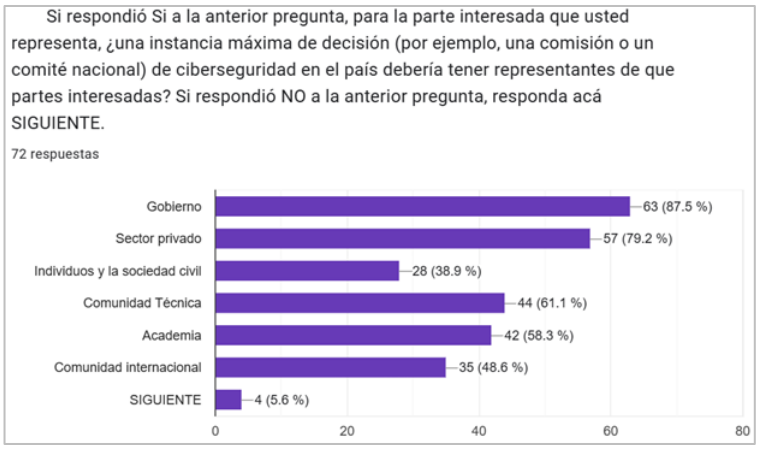
PROPUESTA DE OBJETIVOS Y ACCIONES ESTRATÉGICAS

A continuación, se presenta un ejercicio de validación del marco estratégico basado en las mejores prácticas internacionales y regionales teniendo en cuenta el trabajo con las múltiples partes interesadas en las mesas virtuales y presenciales.

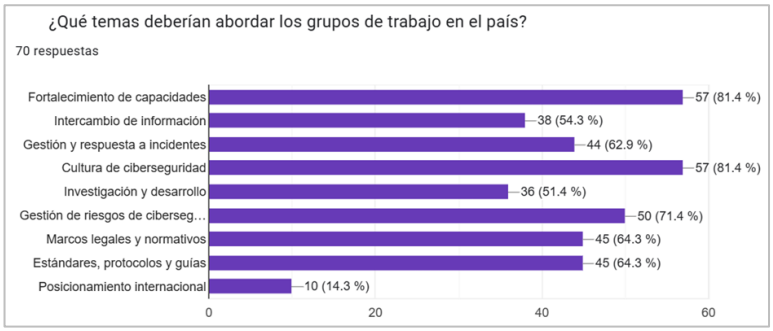
Pilar 1. Gobernanza y Coordinación

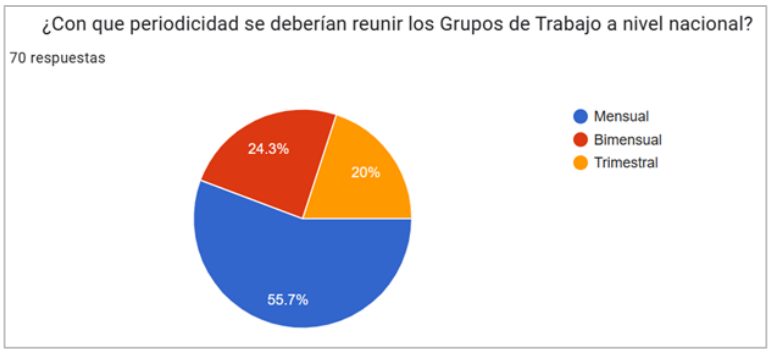
Reforzar la gobernanza de ciberseguridad, optimizando la inversión pública y profundizando en la coordinación entre gobierno, industria, academia, sociedad y comunidad internacional.
Líneas de Acción: • Consolidar la instancia de coordinación nacional de ciberseguridad • Establecer un marco de gobernanza de ciberseguridad de Toda la Sociedad • Asignar eficientemente los recursos para la implementación de iniciativas de ciberseguridad




Si respondió Si a la anterior pregunta, para la parte interesada que usted representa, ¿una instancia máxima de decisión (por ejemplo, una comisión o un comité nacional) de ciberseguridad en el país debería tener representantes de que partes interesadas? Si respondió NO a la anterior pregunta, responda acá SIGUIENTE.
72 respuestas
Gobierno
63 (87.5 %)
Sector privado
57 (79.2 %)
Individuos y la sociedad civil
28 (38.9 %)
Comunidad Técnica
44 (61.1 %)
Academia
42 (58.3 %)
Comunidad internacional
35 (48.6 %)
SIGUIENTE
4 (5.6 %)
0
20
40
60
80


Para la parte interesada que usted representa, ¿Le parecería apropiado la conformación de grupos de trabajo de ciberseguridad en el país que reporten a una instancia de coordinación y a una instancia superior de decisión? Si respondió NO a la anterior pregunta, responda acá FIN y ha terminado la encuesta.
74 respuestas
Si
No
FIN
8.1%
89.2%


¿Qué temas deberían abordar los grupos de trabajo en el país?
70 respuestas
Fortalecimiento de capacidades
57 (81.4 %)
Intercambio de información
38 (54.3 %)
Gestión y respuesta a incidentes
44 (62.9 %)
Cultura de ciberseguridad
57 (81.4 %)
Investigación y desarrollo
36 (51.4 %)
Gestión de riesgos de ciberseg…
50 (71.4 %)
Marcos legales y normativos
45 (64.3 %)
Estándares, protocolos y guías
45 (64.3 %)
Posicionamiento internacional
10 (14.3 %)
0
20
40
60



A continuación, se presenta la valoración de las múltiples partes interesadas respecto de la importancia de las acciones propuestas para reforzar la gobernanza de ciberseguridad en el país, resaltando que han sido catalogadas como urgentes y necesarias.

OBJETIVO ESTRATEGICO	#	LINEA DE ACCIÓN	#	#	INTERVENCIÓN PÚBLICA	Urgente	Necesaria	Postergable	Innecesaria	Total	Urgente	Necesaria	Postergable	Innecesaria	Total
Reforzar la gobernanza de ciberseguridad	1.1	Consolidar la instancia de coordinación nacional de ciberseguridad	1	1.1.1	Hoja de Ruta para reestructurar el MICITT	23	24	11	2	60	38%	40%	18%	3%	100%
			2	1.1.2	Instancia de coordinación nacional de ciberseguridad	27	32	1		60	45%	53%	2%	0%	100%
			3	1.1.3	Recurso humano para la coordinación nacional de ciberseguridad	35	24	1		60	58%	40%	2%	0%	100%
	1.2	Establecer un marco de gobernanza de ciberseguridad de Toda la Sociedad	4	1.2.1	Marco de gobernanza nacional de ciberseguridad	45	14	1		60	75%	23%	2%	0%	100%
			5	1.2.2	Instancia de planeación estratégica de ciberseguridad	19	26	14	1	60	32%	43%	23%	2%	100%
			6	1.2.3	Instancia de planeación táctica de ciberseguridad	24	31	5		60	40%	52%	8%	0%	100%
			7	1.2.4	Mecanismos dinámicos de coordinación y colaboración	28	31	1		60	47%	52%	2%	0%	100%
			8	1.2.5	Figuras de enlace institucional	24	31	5		60	40%	52%	8%	0%	100%
			9	1.2.6	Estrategias, protocolos y mecanismos de comunicación	30	27	3		60	50%	45%	5%	0%	100%
			10	1.2.7	Mecanismos de seguimiento y control	27	30	3		60	45%	50%	5%	0%	100%
			11	1.2.8	Evaluaciones de impacto socio económico	19	27	13	1	60	32%	45%	22%	2%	100%
	1.3	Asignar eficientemente los recursos para la implementación de iniciativas de ciberseguridad	12	1.3.1	Hoja de ruta para la transición al cese de estado de emergencia	19	35	5	1	60	32%	58%	8%	2%	100%
			13	1.3.2	Plan de inversión para iniciativas de ciberseguridad	41	17	2		60	68%	28%	3%	0%	100%
			14	1.3.3	Recurso humano de ciberseguridad en instituciones públicas	46	12	2		60	77%	20%	3%	0%	100%
			15	1.3.4	Presupuesto anual en instituciones públicas	30	24	6		60	50%	40%	10%	0%	100%
			16	1.3.5	Procesos de adquisición y compra de recursos tecnológicos en instituciones públicas	29	26	5		60	48%	43%	8%	0%	100%
			17	1.3.6	Programa de estímulos a la inversión privada	17	30	13		60	28%	50%	22%	0%	100%

Nota: 60 respuestas

A continuación, se analizan los aportes de los participantes en las mesas presenciales en relación con la gobernanza de ciberseguridad y la coordinación en el país.

#	APORTE	CONSIDERACIONES
1	1-Adquisiciones consolidadas de forma eficiente para apalancar economías de escala. 2-Estructuras de gobierno, gestión y operativos ágiles y sectorizadas para atender adecuadamente las necesidades tanto de grandes como pequeños. 3-A nivel técnico y operativo, CSIRT y SOC sectoriales para la orquestación de la defensa y protección.	Se propone: i) desarrollar un plan de inversión que garantice la disponibilidad y asignación de recursos suficientes en instituciones públicas para llevar a cabo iniciativas de ciberseguridad, ii) establecer un marco de gobernanza de ciberseguridad de Toda la Sociedad, iii) crear y ejecutar un plan de fortalecimiento de capacidades operativas, administrativas, humanas, científicas y de

#	APORTE	CONSIDERACIONES
		infraestructura física y tecnológica del Centro de Respuesta de Incidentes de Seguridad Informática (CSIRT-CR) para consolidarlo como equipo de respuesta nacional a incidentes de ciberseguridad, iv) crear y poner en marcha un Centro de Operaciones de Seguridad nacional (SOC-CR) permanente encargado de la gestión preventiva, reactiva y proactiva de riesgos de ciberseguridad a nivel nacional.
2	Actualizar tabla de salarios para atraer personal competente en ciberseguridad. La tabla actual está fuera de toda lógica salarial vigente	Se propone formular e implementar una estrategia de desarrollo de fuerza laboral de ciberseguridad a nivel nacional
3	Adicional a la búsqueda de profesionales en Ciberseguridad, siento que también se debe trabajar fuerte en la retención de ese personal en el sector gobierno, contrario se volverá un trampolín para que profesionales se especialicen y migren al sector privado.	Se propone formular e implementar una estrategia de desarrollo de fuerza laboral de ciberseguridad a nivel nacional
4	Agilizar procesos para el uso efectivo de los recursos	Se propone establecer procesos eficientes para la adquisición y compra de recursos tecnológicos en instituciones públicas para garantizar una gestión integral de los riesgos de ciberseguridad
5	Aportar y dotar de recursos técnicos, financieros a la OSC para desarrollar estrategia de seguimiento y monitoreo de las políticas públicas en ciberseguridad en una interseccionalidad de las publicaciones	Se propone establecer mecanismos de seguimiento y control de indicadores clave de rendimiento y de gestión integral de riesgos de ciberseguridad incluyendo indicadores que contribuyan a medir el impacto de género con perspectiva interseccional.
6	Capacitación	Se propone mejorar y expandir las capacidades y habilidades cibernéticas en todos los niveles en el país
7	Capacitación y Certificaciones	Se propone mejorar y expandir las capacidades y habilidades cibernéticas en todos los niveles en el país
8	Conciencia para directores y políticos	Se propone desarrollar campañas nacionales de concientización sobre la gestión integral de riesgos de ciberseguridad basándose en mejores prácticas dirigida a las múltiples partes interesadas con enfoque de género y con perspectiva interseccional.
9	Concientización de los altos mandos que esto no es algo de TI sino de toda la organización	Se propone desarrollar campañas nacionales de concientización sobre la gestión integral de riesgos de ciberseguridad basándose en mejores prácticas dirigida a las múltiples partes interesadas con enfoque de género y con perspectiva interseccional.
10	Contemplar el enfoque de ciberseguridad como una gestión de gobernanza. El papel de la Cancillería en el ecosistema es muy relevante dada la competencia en los procesos de negociación sobre ciberseguridad y ciberdelincuencia en los foros regionales y multilaterales en curso, así como en la celebración de actos internacionales.	Se propone diseñar y poner en marcha un marco de gobernanza nacional de ciberseguridad promoviendo la participación de las múltiples partes interesadas (incluida la Cancillería), incluyendo autoridades nacionales y organizaciones de sociedad civil que defienden derechos de las personas dadas sus diversas necesidades.
11	Continuidad de programas educativos de prevención.	Se propone mejorar y expandir las capacidades y habilidades cibernéticas en todos los niveles en el país
12	Coordinación entre todos	Se propone crear y poner en marcha mecanismos dinámicos de coordinación y colaboración intergubernamental e intersectorial vinculando a las múltiples partes interesadas.
13	Creo que el ente encargado de ciberseguridad debería de tener capacitaciones en el área como también, deberían estar preparados a la hora de ir a una institución cuando sucede una incidencia y no solo ir de apoyó moral sin saber que hacer para apoyar	Se propone crear y ejecutar un plan de fortalecimiento de capacidades operativas, administrativas, humanas, científicas y de infraestructura física y tecnológica del Centro de Respuesta de Incidentes de Seguridad Informática (CSIRT-CR) para consolidarlo como equipo de respuesta nacional a incidentes de ciberseguridad.
14	Definitivamente el cambio cultural promoverá la priorización de proyectos impostergables de ciberseguridad	Se propone fomentar una cultura ciudadana responsable en ciberseguridad
15	Difusión de políticas, procedimientos y buenas prácticas enfocadas a Pymes	Se propone elaborar y ejecutar programas de desarrollo de capacidades y habilidades de ciberseguridad para profesionales en organizaciones privadas, haciendo énfasis en MIPYMES.
16	El establecimiento de acuerdos de los tres poderes de la República, a participar en la estrategia de ciberseguridad, crear un análisis de la situación actual de cada institución sus vulnerabilidades y como mitigarlas	Se propone diseñar y poner en marcha un marco de gobernanza nacional de ciberseguridad promoviendo la participación de las múltiples partes interesadas (incluido los 3 poderes de la República), incluyendo autoridades nacionales y organizaciones de sociedad civil que defienden derechos de las personas dadas sus diversas necesidades.
17	Empoderar las áreas de ciberseguridad en el staff de las instituciones para que apoyen en las estrategias de seguridad institucionales en la apertura de nuevos servicios automatizados y el reforzamiento de los existentes, así como al reforzamiento de la cultura de ciberseguridad interna	Se propone reforzar la capacidad de instituciones públicas contando con el recurso humano idóneo, promoviendo la igualdad de género y la diversidad y creando perfiles de puestos especializados en ciberseguridad.
18	Es necesario que tanto el cambio a nivel informático vaya de la mano con la legislación y las leyes del país, ya qué hay una nebulosa que deja el margen de acción a nivel judicial abierto. Recordemos que nuestras leyes son muy antiguas solo hay 4 artículos en el código penal y la ley de trato a los datos personales. Se debe preparar un proyecto de ley que abarque Ciberseguridad y Cibercrimen	Se propone fortalecer el marco legal y regulatorio cibernético del país
19	Es necesario que todo el sector público este estandarizado u homologado en sus herramientas para facilitar el despliegue de respuestas desde el MICITT	Se propone establecer estándares, protocolos y procedimientos técnicos para la prevención, contención, resolución y respuesta a incidentes de ciberseguridad a nivel nacional
20	Establecer un marco de gobierno nacional que insten a que las instituciones inviertan en recurso humano y creen áreas de ciberseguridad, dando herramientas eficaces, donde no se vea la	Se propone desarrollar un plan de inversión que garantice la disponibilidad y asignación de recursos suficientes en instituciones públicas para llevar a cabo iniciativas de ciberseguridad.

#	APORTE	CONSIDERACIONES
	seguridad como un recargo en las áreas de TI sino una necesidad institucional	
21	Establecer un marco de referencia actualizado	Se propone establecer estándares, protocolos y procedimientos técnicos para la prevención, contención, resolución y respuesta a incidentes de ciberseguridad a nivel nacional
22	Establecer un plan de capacitación técnica para las instituciones y funcionarios que están a cargo de la seguridad y ciberseguridad.	Se propone elaborar y ejecutar programas de desarrollo de capacidades y habilidades de ciberseguridad para profesionales en instituciones públicas.
23	Establecer una base actual, alinearse a la estrategia y objetivos de cada organización.	Se propone establecer un marco de gobernanza de ciberseguridad de Toda la Sociedad
24	Explicabilidad, rendición de cuentas, transparencia, investigación, desarrollo, fiscalización	Se propone i) desarrollar estrategias, protocolos y mecanismos de comunicación que promuevan la participación de todas las múltiples partes interesadas, especialmente de la academia y sector privado y que rindan cuentas de la ejecución del plan de acción, y ii) establecer mecanismos de seguimiento y control de indicadores clave de rendimiento y de gestión integral de riesgos de ciberseguridad incluyendo indicadores que contribuyan a medir el impacto de género con perspectiva interseccional.
25	Formalizar los instrumentos y protocolos para acciones dentro de alianza público privadas	Se propone fortalecer las alianzas del sector público con el sector privado, las organizaciones de la sociedad civil y la academia.
26	Fortalecer al ente rector y coordinador para que tenga algún tipo de peso o vinculación en los sectores que no pertenecen al gobierno central. Una estrategia para crear confianza con los entes no obligados	Se propone diseñar y poner en marcha un marco de gobernanza nacional de ciberseguridad promoviendo la participación de las múltiples partes interesadas, incluyendo autoridades nacionales y organizaciones de sociedad civil que defienden derechos de las personas dadas sus diversas necesidades.
27	Generación de procesos transparentes desde su diseño	Se pretende formular una estrategia que proporcione una visión cohesiva y convincente construida con todas las múltiples partes interesadas, incluidos los sectores público y privado, las organizaciones de la sociedad civil, la academia y la comunidad en general, abordando las necesidades y los desafíos únicos de la ciudadanía costarricense, promoviendo la igualdad de oportunidades y la participación inclusiva en las iniciativas de ciberseguridad.
28	Generación y actualización de la legislación	Se propone fortalecer el marco legal y regulatorio cibernético del país
29	Implementación de programas de educación en ciberseguridad básica en escuelas, colegio y la población adulta mayor. Si educamos a los niños estaremos fortaleciendo el futuro factor humano de las empresas en instituciones.	Se propone elaborar e implementar un plan nacional de educación y formación en ciberseguridad en todos los niveles del sistema educativo costarricense y promoviendo el fortalecimiento del currículo considerando contenidos de ciberseguridad y la diversidad, igualdad de género e inclusión social.
30	"Iniciar un programa de concienciación dirigido a Jerarcas.	Se propone desarrollar campañas nacionales de concientización sobre la gestión integral de riesgos de ciberseguridad basándose en mejores prácticas dirigida a las múltiples partes interesadas con enfoque de género y con perspectiva interseccional.
31	Velar por que la Estrategia faculte los proyectos-país requeridos. Es decir, los proyectos deben visualizarse de manera que aun cuando concluya una Administración o Gobierno, los mismos deben estar asegurados en su continuidad"	Se propone diseñar y poner en marcha un marco de gobernanza nacional de ciberseguridad promoviendo la participación de las múltiples partes interesadas, incluyendo autoridades nacionales y organizaciones de sociedad civil que defienden derechos de las personas dadas sus diversas necesidades.
32	Involucramiento de los altos jerarcas para concienciar sobre la importancia de este tema.	Se propone desarrollar campañas nacionales de concientización sobre la gestión integral de riesgos de ciberseguridad basándose en mejores prácticas dirigida a las múltiples partes interesadas con enfoque de género y con perspectiva interseccional.
33	Involucrar a la sociedad civil y que su vos sea escuchada	Se propone diseñar y poner en marcha un marco de gobernanza nacional de ciberseguridad promoviendo la participación de las múltiples partes interesadas, incluyendo autoridades nacionales y organizaciones de sociedad civil que defienden derechos de las personas dadas sus diversas necesidades.
34	Involucrar a los altos jerarcas en mesas de sensibilización para que conozcan la necesidad de su participación activa en ciberseguridad y no como un tema delatado.	Se propone desarrollar campañas nacionales de concientización sobre la gestión integral de riesgos de ciberseguridad basándose en mejores prácticas dirigida a las múltiples partes interesadas con enfoque de género y con perspectiva interseccional.
35	La articulación de todos las partes de forma estratégica. Establecer métodos de educación técnica 3n términos comunes y simples para que todo empresario pueda entender y transmitirlo al personal	Se propone elaborar y ejecutar programas de desarrollo de capacidades y habilidades de ciberseguridad para profesionales en organizaciones privadas, haciendo énfasis en MIPYMES.
36	La creación de alianzas con instituciones autónomas, sector privado entre otras organizaciones, que permitan el fortalecimiento del conocimiento del personal calificado en la toma de acciones en Ciberseguridad, así como en beneficio de la sociedad en general.	Se propone fortalecer las alianzas del sector público con el sector privado, las organizaciones de la sociedad civil y la academia.
37	Los planes son necesarios, sin embargo, la implementación de estos es crucial	Se propone i) desarrollar estrategias, protocolos y mecanismos de comunicación que promuevan la participación de todas las múltiples partes interesadas, especialmente de la academia y sector privado y que rindan cuentas de la ejecución del plan de acción, y ii) establecer mecanismos de seguimiento y control de indicadores clave de rendimiento y de gestión integral de riesgos de ciberseguridad incluyendo indicadores que contribuyan a medir el impacto de género con perspectiva interseccional.

#	APORTE	CONSIDERACIONES
38	Me gustaría alguna legislación que aplique presión política a los jerarcas de las instituciones, relacionado a mantener personal de ciberseguridad capacitado, las 24h, recurso humano mínimo para el área, entre otros.	Se propone fortalecer el marco normativo técnico relacionado con la gestión integral de riesgos de ciberseguridad
39	Mecanismos de retención de personal calificado en ciberseguridad para las empresas públicas	Se propone formular e implementar una estrategia de desarrollo de fuerza laboral de ciberseguridad a nivel nacional
40	Minimizar por medio aportes a la concientización y conocimiento base a la población de poco acceso a la tecnología. Esto por cuanto pueden conocer el uso de esta mas no de ciberseguridad o seguridad de la información.	Se propone elaborar y ejecutar programas de desarrollo de capacidades y habilidades de ciberseguridad para la sociedad costarricense en general reconociendo las necesidades de seguridad diferenciadas e interseccionales de las personas y comunidades.
41	Obligatoriedad de instancias técnicas de ciberseguridad con sus roles y potestades dentro de la organización.	Se propone apoyar a los reguladores sectoriales en el ejercicio de supervisión y verificación del cumplimiento de las disposiciones de los marcos regulatorios sectoriales relacionadas con la ciberseguridad.
42	Plan sostenible a mediano-largo plazo, sujeto a cambios legales y administrativos según los avances tecnológicos.	Se propone i) desarrollar estrategias, protocolos y mecanismos de comunicación que promuevan la participación de todas las múltiples partes interesadas, especialmente de la academia y sector privado y que rindan cuentas de la ejecución del plan de acción, y ii) establecer mecanismos de seguimiento y control de indicadores clave de rendimiento y de gestión integral de riesgos de ciberseguridad incluyendo indicadores que contribuyan a medir el impacto de género con perspectiva interseccional.
43	Que el MICITT de verdad tome la batuta que le corresponde	Se propone fortalecer la instancia de coordinación nacional para dirigir la implementación de la Estrategia Nacional de Ciberseguridad 2023-2027 y hacer seguimiento continuo, dotándola de herramientas jurídicas y técnicas que le permitan desempeñar sus funciones con la mayor efectividad
44	Que las instituciones desarrollen sus Marcos normativos de ciberseguridad para facilitar la integración del plan. Se quiere integrar un SOC pero existe la clasificación de la información, hay activos críticos definidos en la institución? Son retos que tienen las instituciones públicas. Cada sector es diferente y sus necesidades también. Se debe normar a las instituciones públicas a nivel de ley para cumplir y no se quede en papel.	Se propone i) fortalecer el marco normativo técnico relacionado con la gestión integral de riesgos de ciberseguridad, y ii) fortalecer las capacidades nacionales de monitoreo, detección y respuesta a incidentes de ciberseguridad
45	Que los actores claves (profesión de Ciberseguridad) de las instituciones se les del rol que corresponde (puesto y salario) y así se mantengan en las instituciones públicas, para que los esfuerzos en trabajos no se pierdan	Se propone formular e implementar una estrategia de desarrollo de fuerza laboral de ciberseguridad a nivel nacional
46	Reestructurar las organizaciones para que las unidades de TI se promuevan a Direcciones para impactar en la toma de decisiones de seguridad ciberseguridad y la gestión en general de TI.	Se propone i) desarrollar un plan de inversión que garantice la disponibilidad y asignación de recursos suficientes en instituciones públicas para llevar a cabo iniciativas de ciberseguridad, y ii) promover en las instituciones públicas a contar con recursos financieros presupuestando anualmente aquellos necesarios para la gestión integral de riesgos de ciberseguridad.
47	Se deben de establecer una cultura de colaboración práctica y sencilla entre sectores (Gobierno, Banca, sector privado, gobiernos locales, autónomas, academia). Por ejemplo, elaborar estándares que se pongan al servicio de todos con elementos por nivel de madurez (básico, intermedio y avanzando) y que una Institución tenga un punto de inicio donde exista participación de los sectores para construir un ecosistema seguro sea en el GAM o en una Municipalidad rural. Hay realidades diferentes en estos 51.100 km2	Se propone crear y poner en marcha mecanismos dinámicos de coordinación y colaboración intergubernamental e intersectorial vinculando a las múltiples partes interesadas.
48	Si, educacional.	Se propone mejorar y expandir las capacidades y habilidades cibernéticas en todos los niveles en el país
49	Siempre hay espacio para la mejora, sin embargo, hasta no comenzar y validar, no tengo nada que agregar…	Se proponen acciones que se dedican a todos los sectores de la economía y la sociedad, desde las instituciones de la administración pública central hasta los líderes de toda la industria y la ciudadanía, con el fin de alcanzar objetivos estratégicos y el objetivo general
50	Tener una estrategia clara y ejecutable que pueda pasar del papel a la acción con facilidad y que no tenga muchos obstáculos para su implementación	Se propone i) desarrollar estrategias, protocolos y mecanismos de comunicación que promuevan la participación de todas las múltiples partes interesadas, especialmente de la academia y sector privado y que rindan cuentas de la ejecución del plan de acción, y ii) establecer mecanismos de seguimiento y control de indicadores clave de rendimiento y de gestión integral de riesgos de ciberseguridad incluyendo indicadores que contribuyan a medir el impacto de género con perspectiva interseccional.
51	Todas estas cosas son relevantes, pero creo que lo que hay que hacer de primero es establecer los servicios esenciales y de allí comprender el estado de la protección de la información y su infraestructura crítica asociada.	Se propone i) definir y evaluar periódicamente los criterios para designar infraestructuras críticas nacionales teniendo en cuenta la protección de los derechos humanos de las personas dadas sus diversas necesidades, ii) identificar a los operadores que ejercen el control sobre las infraestructuras críticas nacionales y prestan servicios esenciales, y iii) identificar y categorizar las infraestructuras críticas nacionales.
52	Tomar en cuenta que las estructuras burocráticas en aspectos técnicos suelen extender las limitaciones y convertirse en un "fin en si mismo",	Se propone diseñar y poner en marcha un marco de gobernanza nacional de ciberseguridad promoviendo la participación de las múltiples partes interesadas, incluyendo autoridades nacionales y

#	APORTE	CONSIDERACIONES
	donde el aporte es siempre gubernamental sin representar a la sociedad en general	organizaciones de sociedad civil que defienden derechos de las personas dadas sus diversas necesidades.
53	Trabajar con sociedad civil, e instituciones de infraestructura crítica	Se propone diseñar y poner en marcha un marco de gobernanza nacional de ciberseguridad promoviendo la participación de las múltiples partes interesadas, incluyendo autoridades nacionales y organizaciones de sociedad civil que defienden derechos de las personas dadas sus diversas necesidades.
54	Una mejor integración del gobierno junto con el sector privado	Se propone fortalecer las alianzas del sector público con el sector privado, las organizaciones de la sociedad civil y la academia
55	Velar por la calidad de la educación qué se imparte en ciberseguridad, contar con guías de implementación de la ciberseguridad en las instituciones	Se propone establecer guías, estándares, protocolos y procedimientos técnicos para la prevención, contención, resolución y respuesta a incidentes de ciberseguridad a nivel nacional.

Pilar 2. Marco legal y regulatorio

Adecuar el marco jurídico cibernético, promoviendo una cultura de cumplimiento y considerando las amenazas cibernéticas en evolución, los avances tecnológicos y las necesidades únicas de la Nación

Líneas de Acción:

- Fortalecer el marco legal y regulatorio cibernético
- Fortalecer el marco normativo técnico relacionado con la gestión integral de riesgos de ciberseguridad

A continuación, se presenta la valoración de las múltiples partes interesadas respecto de la importancia de las acciones propuestas para adecuar el marco jurídico cibernético en el país, resaltando que han sido catalogadas como urgentes y necesarias.

OBJETIVO ESTRATEGICO	#	LINEA DE ACCIÓN	#	#	INTERVENCIÓN PÚBLICA	Urgente	Necesaria	Postergable	Innecesaria	Total	Urgente	Necesaria	Postergable	Innecesaria	Total
Adecuar el marco jurídico cibernético	2.1	Fortalecer el marco legal y regulatorio cibernético	18	2.1.1	Trámites de iniciativas o proyectos legislativos	23	28	3	1	55	42%	51%	5%	2%	100%
			19	2.1.2	Trámite de iniciativas o proyectos regulatorios	24	28	3		55	44%	51%	5%	0%	100%
			20	2.1.3	Revisión del marco legal y regulatorio cibernético	42	11	2		55	76%	20%	4%	0%	100%
	2.2	Fortalecer el marco normativo técnico relacionado con la gestión integral de riesgos de ciberseguridad	21	2.2.1	Marco normativo del CSIRT-CR	22	25	7	1	55	40%	45%	13%	2%	100%
			22	2.2.2	Estándares, protocolos y procedimientos técnicos: Guías y Plan	37	15	3		55	67%	27%	5%	0%	100%
			23	2.2.3	Marco normativo para la protección de infraestructuras críticas nacionales y de operadores de servicios esenciale	37	14	3	1	55	67%	25%	5%	2%	100%
			24	2.2.4	Mecanismos de supervisión al cumplimiento	26	24	5		55	47%	44%	9%	0%	100%

Nota: 55 respuestas

A continuación, se analizan los aportes de los participantes en las mesas presenciales en relación con el marco jurídico cibernético en el país.

#	APORTE	CONSIDERACIONES
56	Capacitación	Se propone mejorar y expandir las capacidades y habilidades cibernéticas en todos los niveles en el país
57	1-El gobierno de la seguridad debe coordinar con el gobierno corporativa la definición de activos críticos de información a partir de servicios críticos del negocio. En la coyuntura, el gobierno corporativo es en ocasiones periféricos o ausente de la dinámica digital.	Se propone i) definir y evaluar periódicamente los criterios para designar infraestructuras críticas nacionales teniendo en cuenta la protección de los derechos humanos de las personas dadas sus diversas necesidades, ii) identificar a los operadores que ejercen el control sobre las infraestructuras críticas nacionales y prestan servicios esenciales, y iii) identificar y categorizar las infraestructuras críticas nacionales
58	Adecuar INTEGRALMENTE todos los marcos normativos que inciden en la materia.	Se propone desarrollar legislación y regulación cibernética junto con un marco normativo técnico para la ciberseguridad
59	Básicamente esas.	-
60	Benchmarking con países avanzados en el tema	Se propone desarrollar un marco normativo para la protección de infraestructuras críticas nacionales y de operadores de servicios esenciales, adoptando normas y estándares internacionales
61	Capacitaciones y mesas de trabajo	Se propone diseñar y poner en marcha un marco de gobernanza nacional de ciberseguridad promoviendo la participación de las múltiples partes interesadas, incluyendo autoridades nacionales y organizaciones de sociedad civil que defienden derechos de las personas dadas sus diversas necesidades.
62	Como se dice en una de las preguntas, es de vital importancia crear un proyecto de ley que contemple el presupuesto que se vaya a necesitar y además la importancia de la creación de la ley de ciberseguridad con su capítulo de penalización al no cumplirse cuando hay un cibercrimen o ciberataque.	Se propone apoyar a la Asamblea Legislativa en el trámite de iniciativas o proyectos para adecuar, adaptar y/o armonizar el marco legal relacionado con la ciberseguridad.
63	Conformar un equipo donde haya una representación de las áreas involucradas para adecuar el marco normativo con empatía conforme las necesidades.	Se propone diseñar y poner en marcha un marco de gobernanza nacional de ciberseguridad promoviendo la participación de las múltiples partes interesadas, incluyendo autoridades nacionales y organizaciones de sociedad civil que defienden derechos de las personas dadas sus diversas necesidades.
64	Consulta pública	Se propone adelantar un proceso de consulta pública oficial de la Estrategia Nacional de Ciberseguridad
65	Contratar más personal capacitado.	Se propone reforzar la capacidad de instituciones públicas contando con el recurso humano idóneo, promoviendo la igualdad de género y la diversidad y creando perfiles de puestos especializados en ciberseguridad.
66	Crear un análisis integral la ciberseguridad, los marcos y modelos a seguir, ISO 27001 y 23001, NIS... Cuál debe ser el organigrama institucional de cara la Ciberseguridad	Se propone establecer estándares, protocolos y procedimientos técnicos para la prevención, contención, resolución y respuesta a incidentes de ciberseguridad a nivel nacional
67	Dar prioridad a los procesos de comunicación con los altos jerarcas	Se propone desarrollar estrategias, protocolos y mecanismos de comunicación que promuevan la participación de todas las múltiples partes interesadas, especialmente de la academia y sector privado y que rindan cuentas de la ejecución del plan de acción.
68	"Debe partirse por definir ámbitos de acción y a partir de ahí, gestionar el riesgo.	Se propone establecer un marco de gestión integral de riesgos de ciberseguridad que permita la detección, el reporte, el análisis y la respuesta oportuna a incidentes de ciberseguridad.
69	Una infraestructura puede no ser crítica a nivel nacional, pero igual si es afectada impactará al sector al cual pertenece y a quienes se relacionan con ella."	Se propone i) definir y evaluar periódicamente los criterios para designar infraestructuras críticas nacionales teniendo en cuenta la protección de los derechos humanos de las personas dadas sus diversas necesidades, ii) identificar a los operadores que ejercen el control sobre las infraestructuras críticas nacionales y prestan servicios esenciales, y iii) identificar y categorizar las infraestructuras críticas nacionales
70	Definir la hoja de ruta de atención institucional, según procedimientos, y normativa definida como de cumplimiento	Se propone establecer estándares, protocolos y procedimientos técnicos para la prevención, contención, resolución y respuesta a incidentes de ciberseguridad a nivel nacional
71	Definir marco regulatorio y plan de acción	Se propone desarrollar legislación y regulación cibernética junto con un marco normativo técnico para la ciberseguridad
72	Definir requerimientos y alcances para que se pueda alcanzar a todas las organizaciones sin importar si es público o privada tales como la protección de datos y privacidad. Que por ley se de importancia al área de seguridad debido a que puede haber conflictos de interés según diagrama institucional.	Se propone revisar y actualizar integralmente el marco legal y regulatorio cibernético haciendo énfasis en la protección legal contra las amenazas cibernéticas basadas en género con perspectiva interseccional, previniendo, sancionando y erradicando la violencia de género facilitada por las tecnologías digitales.
73	Enfatizar políticas paralelas, comunicaciones y retroalimentación. Líneas directas de mando en Costa Rica son poca realistas ante la separación de poderes y autónomas.	Se propone diseñar y poner en marcha un marco de gobernanza nacional de ciberseguridad promoviendo la participación de las múltiples partes interesadas, incluyendo autoridades nacionales y organizaciones de sociedad civil que defienden derechos de las personas dadas sus diversas necesidades.
74	Es necesario crear leyes de protección de datos que realmente protejan al ciudadano	Se propone apoyar a la Asamblea Legislativa en el trámite de iniciativas o proyectos para adecuar, adaptar y/o armonizar el marco legal relacionado con la ciberseguridad.
75	Es necesario que las personas desde sus niveles educativos inferiores puedan tener una formación de la normativa que se impulsa para regular y sancionar todo lo relacionado con los ciberdelitos de forma tal que su incidencia sea menor contrario a lo que sucede en el presente	Se propone impulsar el cumplimiento del marco normativo técnico relacionado con la gestión integral de riesgos de ciberseguridad

#	APORTE	CONSIDERACIONES
76	Es urgente actualizar la normativa nacional para que el MICITT como ente rector tenga músculo para gestionar y solicitar cumplimientos bajo el Marco de ciberseguridad	Se propone actualizar el marco normativo para fortalecer los procesos de gestión administrativa y técnica del Centro de Respuesta de Incidentes de Seguridad Informática (CSIRT-CR).
77	Establecer estándares, protocolos y procedimientos técnicos para la prevención, contención, resolución y respuesta a incidentes	Se propone establecer estándares, protocolos y procedimientos técnicos para la prevención, contención, resolución y respuesta a incidentes de ciberseguridad a nivel nacional
78	Establecer la línea base.	Se propone establecer mecanismos de seguimiento y control de indicadores clave de rendimiento y de gestión integral de riesgos de ciberseguridad incluyendo indicadores que contribuyan a medir el impacto de género con perspectiva interseccional.
79	Establecer qué el cumplimiento de esos marcos normativos sea obligatorio y que sea obligatorio que una entidad qué ha sufrido un evento adverso de ciberseguridad lo publique, esto para darle confianza al usuario sobre la seguridad en el servicio que está utilizando	Se propone apoyar a los reguladores sectoriales en el trámite de iniciativas o proyectos para adecuar, adaptar y/o armonizar el marco regulatorio relacionado con la ciberseguridad, así como en el ejercicio de supervisión y verificación del cumplimiento de las disposiciones de los marcos regulatorios sectoriales relacionadas con la ciberseguridad.
80	Estandarizar el Marco Normativo para todo el sector público	Se propone asegurar la existencia de marcos legales y regulatorios robustos para promover la gestión integral de riesgos de ciberseguridad y hacer frente a las ciber amenazas.
81	Flexibilización en las contrataciones, ya que aún y cuando se tenga el presupuesto y la identificación del tema como un riesgo, se tienen trabas para poder gestionar los contratos. El decreto de emergencia es muy general, debía ser más claro.	Se propone establecer procesos eficientes para la adquisición y compra de recursos tecnológicos en instituciones públicas para garantizar una gestión integral de los riesgos de ciberseguridad.
82	Fomentar el marco jurídico dentro de las mismas instituciones gubernamentales	Se propone impulsar el cumplimiento del marco normativo técnico relacionado con la gestión integral de riesgos de ciberseguridad.
83	Fortalecer el marco regulatorio nacional para un por lado priorizar la gestión de recursos hacia la protección de infraestructura crítica y por otro lado homogeneizar las capacidades de las diferentes unidades/instituciones gubernamentales para hacer frente a los riesgos en ciberseguridad	Se propone desarrollar un marco normativo para la protección de infraestructuras críticas nacionales y de operadores de servicios esenciales, adoptando normas y estándares internacionales
84	Fortalecer las unidades judiciales para la atención, investigación y judicialización de los delitos cibernéticos	Se propone i) reforzar la capacidad de instituciones públicas contando con el recurso humano idóneo, promoviendo la igualdad de género y la diversidad y creando perfiles de puestos especializados en ciberseguridad, y ii) promover en las instituciones públicas a contar con recursos financieros presupuestando anualmente aquellos necesarios para la gestión integral de riesgos de ciberseguridad.
85	Generar una rendición de cuentas	Se propone desarrollar estrategias, protocolos y mecanismos de comunicación que promuevan la participación de todas las múltiples partes interesadas, especialmente de la academia y sector privado y que rindan cuentas de la ejecución del plan de acción.
86	"La existencia de Mejores Prácticas no requiere legislaciones si son buenas. ¡¡¡Lo que importa es tener la definición de las prácticas y sobre todo definir que queremos proteger!!!	Se propone i) definir y evaluar periódicamente los criterios para designar infraestructuras críticas nacionales teniendo en cuenta la protección de los derechos humanos de las personas dadas sus diversas necesidades, ii) identificar a los operadores que ejercen el control sobre las infraestructuras críticas nacionales y prestan servicios esenciales, y iii) identificar y categorizar las infraestructuras críticas nacionales.
87	La normativa debe armonizarse con el marco de derechos humanos adoptado por el país mediante otros instrumentos. También incluir la urgencia de contar con normativa moderna y clara en el campo de protección de privacidad y datos necesarios porque actualmente se tienen muchos vacíos que llevan a abusos y vocación de derechos de la ciudadanía	Se propone desarrollar legislación y regulación cibernética junto con un marco normativo técnico para la ciberseguridad con enfoque de Derechos Humanos y enfoque centrado en el ser humano, aplicando principios orientadores como el respeto a los Derechos Humanos y los valores fundamentales
88	La regulación debe ser integral y debe estar en función de lo que necesita el país, se debe analizar si toda la normativa que está actualmente vigente cubre las necesidades reales o si se deben derogar o eliminar las que ya no sean tel antes o copias de normativa internacional que puede usarse como referencia sin necesidad de que se "creen" nuevas normativas que son copias de las normas internacionales	Se propone revisar y actualizar integralmente el marco legal y regulatorio cibernético haciendo énfasis en la protección legal contra las amenazas cibernéticas basadas en género con perspectiva interseccional, previniendo, sancionando y erradicando la violencia de género facilitada por las tecnologías digitales.
89	Legislación que obligue a las instituciones a cumplir con algunos requisitos básicos de ciberseguridad, como lo son los recursos	Se propone asegurar la existencia de marcos legales y regulatorios robustos para promover la gestión integral de riesgos de ciberseguridad y hacer frente a las ciber amenazas.
90	Marco regulatorio que permita sancionar a jerarcas por incumplir lo dispuesto en materia de seguridad ciberseguridad	Se propone asegurar la existencia de marcos legales y regulatorios robustos para promover la gestión integral de riesgos de ciberseguridad y hacer frente a las ciber amenazas.
100	Ordenar posibles inconsistencias legales existentes	Se propone asegurar la existencia de marcos legales y regulatorios robustos para promover la gestión integral de riesgos de ciberseguridad y hacer frente a las ciber amenazas.
101	Se deben de establecer un marco normativo práctico que sea realizable. Muchas veces se desarrollan marcos que son deseos y aspiraciones que en ocasiones no son implementarles, por eso considero que debemos buscar ser prácticos	Se propone fortalecer el marco normativo técnico relacionado con la gestión integral de riesgos de ciberseguridad

#	APORTE	CONSIDERACIONES
102	Un análisis a sobre las principales amenazas a nivel cibernético y las carencias a nivel jurídico-penal en todas aquellas conductas que pueden ser consideradas como sancionables o punibles.	Se propone revisar y actualizar integralmente el marco legal y regulatorio cibernético haciendo énfasis en la protección legal contra las amenazas cibernéticas basadas en género con perspectiva interseccional, previniendo, sancionando y erradicando la violencia de género facilitada por las tecnologías digitales.
103	Unificar normas y estándares	Se propone desarrollar estrategias, protocolos y mecanismos de comunicación que promuevan la participación de todas las múltiples partes interesadas, especialmente de la academia y sector privado y que rindan cuentas de la ejecución del plan de acción.
104	Urge una sincronía entre las necesidades de ciberseguridad del país y la generación de una normativa que lo permita	Se propone revisar y actualizar integralmente el marco legal y regulatorio cibernético haciendo énfasis en la protección legal contra las amenazas cibernéticas basadas en género con perspectiva interseccional, previniendo, sancionando y erradicando la violencia de género facilitada por las tecnologías digitales.

Pilar 3. Protección de infraestructuras y ciber resiliencia

Fortalecer la protección de infraestructuras y la ciber resiliencia nacional, protegiendo las infraestructuras críticas nacionales y gestionando adecuadamente los riesgos de ciberseguridad para que las partes interesadas puedan maximizar los beneficios del entorno digital y la ciudadanía esté más segura en línea

Líneas de Acción:

- Adoptar un marco para la gestión integral de riesgos de ciberseguridad
- Fortalecer las capacidades nacionales de monitoreo, detección y respuesta a incidentes de ciberseguridad
- Proteger y defender las infraestructuras críticas nacionales y los operadores de servicios esenciales
- Fortalecer el tratamiento de la información relacionada con incidentes de ciberseguridad

A continuación, se presenta la valoración de las múltiples partes interesadas respecto de la importancia de las acciones propuestas para fortalecer la protección de infraestructuras y la ciber resiliencia nacional, resaltando que han sido catalogadas como urgentes y necesarias.

OBJETIVO ESTRATEGICO	#	LINEA DE ACCIÓN	#	#	INTERVENCIÓN PÚBLICA	Urgente	Necesaria	Postergable	Innecesaria	Total	Urgente	Necesaria	Postergable	Innecesaria	Total
Fortalecer la protección de infraestructuras y la ciber resiliencia nacional	3.1	Adoptar un marco para la gestión integral de riesgos de ciberseguridad	25	3.1.1	Marco de gestión integral de riesgos de ciberseguridad	47	16	3		66	71%	24%	5%	0%	100%
			26	3.1.2	Procesos de seguimiento y revisión periódica a la implementación del marco de gestión integral de riesgos	20	42	4		66	30%	64%	6%	0%	100%
			27	3.1.3	Integración de la gestión de riesgos de ciberseguridad en procesos institucionales	41	23	2		66	62%	35%	3%	0%	100%
	3.2	Fortalecer las capacidades nacionales de monitoreo, detección y respuesta a incidentes de ciberseguridad	28	3.2.1	Plan de fortalecimiento de capacidades de CSRT-CR	30	35	1		66	45%	53%	2%	0%	100%
			29	3.2.2	Solución de Centro de Operaciones de Seguridad (SOC)	28	36	2		66	42%	55%	3%	0%	100%
			30	3.2.3	Instituciones públicas priorizadas	38	28			66	58%	42%	0%	0%	100%
			31	3.2.4	Centro de Operaciones de Seguridad nacional (SOC-CR) permanente	29	32	5		66	44%	48%	8%	0%	100%
			32	3.2.5	Sistemas avanzados de alerta y respuesta intersectorial	37	28	1		66	56%	42%	2%	0%	100%
			33	3.2.6	Estrategia para promover SOC sectoriales	29	33	3	1	66	44%	50%	5%	2%	100%
	3.3	Proteger y defender las infraestructuras críticas nacionales y los operadores de servicios esenciales	34	3.3.1	Criterios para designar infraestructuras críticas nacionales	28	33	5		66	42%	50%	8%	0%	100%
			35	3.3.2	Identificación de operadores de infraestructuras críticas nacionales y que prestan servicios esenciales	34	29	3		66	52%	44%	5%	0%	100%
			36	3.3.3	Catálogo de infraestructuras críticas nacionales	47	17	2		66	71%	26%	3%	0%	100%
			37	3.3.4	Evaluaciones de riesgos de ciberseguridad de infraestructuras críticas nacionales	32	34			66	48%	52%	0%	0%	100%
			38	3.3.5	Ejercicios y simulacros nacionales de ciberseguridad	21	38	6	1	66	32%	58%	9%	2%	100%
	3.4	Fortalecer el tratamiento de la información relacionada con incidentes de ciberseguridad	39	3.4.1	Registro Nacional de Incidentes de Ciberseguridad	17	43	6		66	26%	65%	9%	0%	100%
			40	3.4.2	Mecanismos eficientes para el tratamiento de la información de incidentes de ciberseguridad	24	39	3		66	36%	59%	5%	0%	100%
			41	3.4.3	Mecanismo de notificación a autoridades del cumplimiento de la ley	18	38	10		66	27%	58%	15%	0%	100%
			42	3.4.4	Mecanismo de notificación a personas u organizaciones afectadas	24	35	7		66	36%	53%	11%	0%	100%
			43	3.4.5	Mecanismo de divulgación de información sobre riesgos de ciberseguridad	33	32	1		66	50%	48%	2%	0%	100%

Nota: 66 respuestas

A continuación, se analizan los aportes de los participantes en las mesas presenciales en relación con la protección de infraestructuras y la ciber resiliencia nacional.

#	APORTE	CONSIDERACIONES
105	1-Articular con el Gobierno corporativo la figura del CISO en todas las instituciones para el adecuado manejo de las políticas, gestiones y operativa.	Se propone crear una figura de enlace (persona responsable de ciberseguridad) en instituciones públicas, en gobiernos locales y en otras organizaciones a nivel operativo.
106	Al respecto del punto 5 no se trata de crear más órganos burocráticos sino al contrario se necesita acuerpar al CSIRT de herramientas tecnológicas avanzadas que permitan actuar reactiva mente en la infraestructura país	Se propone crear y ejecutar un plan de fortalecimiento de capacidades operativas, administrativas, humanas, científicas y de infraestructura física y tecnológica del Centro de Respuesta de Incidentes de Seguridad Informática (CSIRT-CR) para consolidarlo como equipo de respuesta nacional a incidentes de ciberseguridad.
107	Apoyo o soporte a entidades con pocos recursos, asociaciones, fundaciones, etc. que necesitan apoyo en ciber resiliencia	Se propone i) desarrollar un plan de inversión que garantice la disponibilidad y asignación de recursos suficientes en instituciones públicas para llevar a cabo iniciativas de ciberseguridad, ii) reforzar la capacidad de instituciones públicas contando con el recurso humano idóneo, promoviendo la igualdad de género y la diversidad y creando perfiles de puestos especializados en ciberseguridad, y iii) promover en las instituciones públicas a contar con recursos financieros presupuestando anualmente aquellos necesarios para la gestión integral de riesgos de ciberseguridad.
108	Básicamente esas.	-
109	Campañas anti Ransomware	Se propone establecer guías para reducir el impacto y la probabilidad de incidentes de ransomware y extorsión de datos en organizaciones públicas y privadas, incluyendo mejores prácticas internacionales para prepararse, prevenir y mitigar estos incidentes.
110	Capacitación	Se propone mejorar y expandir las capacidades y habilidades cibernéticas en todos los niveles en el país
111	Capacitación y concientización sobre Ciberseguridad	Se propone mejorar y expandir las capacidades y habilidades cibernéticas en todos los niveles en el país
112	Capacitación y sensibilización	Se propone mejorar y expandir las capacidades y habilidades cibernéticas en todos los niveles en el país
113	Capacitaciones	Se propone mejorar y expandir las capacidades y habilidades cibernéticas en todos los niveles en el país
114	Capacitar a la parte de auditoría a realizar el trabajo enfocado a ciberseguridad	Se pretende formular e implementar una estrategia de desarrollo de fuerza laboral de ciberseguridad a nivel nacional atendiendo las necesidades del mercado laboral y las tendencias en

#	APORTE	CONSIDERACIONES
		ciberseguridad, así como promoviendo la diversidad, igualdad de género e inclusión social.
115	Capacitar al personal informático de las instituciones públicas, en temas de prevención y soluciones de ciberseguridad	Se propone elaborar y ejecutar programas de desarrollo de capacidades y habilidades de ciberseguridad para profesionales y altas y altos jerarcas en instituciones públicas.
116	Como participante del sector financiero creo muy importante la creación de un SOC sectorial, que alimente un SOC nacional. Hago hincapié de la creación de un SOC sectorial pues las necesidades, requerimientos y experiencias de cada sector son muy diferentes, y el SOC debe cumplir esas necesidades específicas e igualmente contribuir a un SOC nacional	Se propone crear y ejecutar una estrategia para promover la creación y el fortalecimiento de SOC sectoriales.
117	Conocer el estado actual de las instituciones en temas de Ciber y a partir de allí, crear el plan estratégico y este implementarlo	Se propone adelantar evaluaciones de riesgos de ciberseguridad de las infraestructuras críticas nacionales en conjunto con los operadores de servicios esenciales.
118	Considero importante utilizar todos los medios de comunicación existente para la ciudadanía (TV, radio). No todos tienen la capacidad de tener una computadora. Usar canales de las redes sociales para fomentar una cultura de ciberseguridad a nivel nacional. Al menos básico.	Se propone desarrollar estrategias, protocolos y mecanismos de comunicación que promuevan la participación de todas las múltiples partes interesadas, especialmente de la academia y sector privado y que rindan cuentas de la ejecución del plan de acción.
119	Coordinar para que exista la cooperación y comunicación interinstitucional entre las instituciones para que la información sobre todo lo relacionado a Ciberseguridad se encuentra a la mano de cada una y esta pueda acoplarlo según sus necesidades o problemáticas.	Se propone promover la celebración de iniciativas de cooperación, colaboración y asistencia intergubernamental e intersectorial.
120	Crear campañas anti-phishing en compañías	Se propone i) desarrollar campañas nacionales de concientización sobre la gestión integral de riesgos de ciberseguridad basándose en mejores prácticas dirigida a las múltiples partes interesadas con enfoque de género y con perspectiva interseccional, ii) desarrollar herramientas y recursos en línea, como tutoriales, videos y guías, que permitan a la ciudadanía costarricense adquirir y fortalecer habilidades en ciberseguridad, y iii) crear un programa de concientización en prácticas de ciberhigiene y uso responsable de la tecnología para la población en general, y para las infancias y adolescencias en particular.
121	Crear espacios seguros y de confianza intersectoriales para el intercambio de información sobre amenazas e incidentes de ciberseguridad. Establecer en el ente competente una estrategia y desarrollar las capacidades de Ciber inteligencia que permita anticipar las amenazas contra infraestructura crítica del país	Se propone i) crear y poner en marcha mecanismos dinámicos de coordinación, y colaboración e intercambio de información intergubernamental e intersectorial vinculando a las múltiples partes interesadas, y ii) crear un Registro Nacional de Incidentes de Ciberseguridad haciendo énfasis en el reporte de incidentes de ciberseguridad en infraestructuras críticas nacionales.
122	Crear registros no solo de autoridades responsables de servicios críticos sino de operadores, incluyendo un registro estricto de equipos que están en ubicaciones privadas por teletrabajo u otros motivos.	Se propone crear un Registro Nacional de Incidentes de Ciberseguridad haciendo énfasis en el reporte de incidentes de ciberseguridad en infraestructuras críticas nacionales
123	Crear una cultura de orientación y educación en ciberseguridad para las empresas y población civil	Se propone desarrollar campañas nacionales de concientización sobre la gestión integral de riesgos de ciberseguridad basándose en mejores prácticas dirigida a las múltiples partes interesadas con enfoque de género y con perspectiva interseccional.
124	Crear y ejecutar un plan de fortalecimiento de capacidades operativas, administrativas, humanas, científicas y de infraestructura física y Tecnológica para las instituciones del poder ejecutivo.	Se propone i) crear y ejecutar un plan de fortalecimiento de capacidades operativas, administrativas, humanas, científicas y de infraestructura física y tecnológica del Centro de Respuesta de Incidentes de Seguridad Informática (CSIRT-CR) para consolidarlo como equipo de respuesta nacional a incidentes de ciberseguridad, ii) desarrollar un plan de inversión que garantice la disponibilidad y asignación de recursos suficientes en instituciones públicas para llevar a cabo iniciativas de ciberseguridad, iii) reforzar la capacidad de instituciones públicas contando con el recurso humano idóneo, promoviendo la igualdad de género y la diversidad y creando perfiles de puestos especializados en ciberseguridad, y iv) promover en las instituciones públicas a contar con recursos financieros presupuestando anualmente aquellos necesarios para la gestión integral de riesgos de ciberseguridad.
125	De momento ninguna otra acción	-
126	Debe existir una alianza real entre el sector público/privado donde se puede contribuir de forma más ágil los servicios orientados a la gestión de riesgos, SOC, a través de empresas con amplia experiencia en estos temas.	Se propone fortalecer las alianzas del sector público con el sector privado, las organizaciones de la sociedad civil y la academia.
127	Definición de un marco básico de aplicación de controles por sector. Del lado público obligatorio y del lado privado con oportunidad de certificación (tener un sello de certificación para tal sector)	Se propone i) elaborar un marco de gestión integral de riesgos de ciberseguridad a nivel nacional incorporando el enfoque de género con perspectiva interseccional para proteger los derechos de las personas dadas sus diversas necesidades, ii) establecer procesos de seguimiento y revisión periódica a la implementación del marco de gestión integral de riesgos de ciberseguridad adaptándolo a las nuevas amenazas, vulnerabilidades y tendencias en el ámbito de la ciberseguridad, y iii) garantizar que los procesos de gestión de riegos de ciberseguridad y de gestión de riesgos de la seguridad de la información se integren en los procesos de planificación

#	APORTE	CONSIDERACIONES
		estratégica, operativa, y presupuestaria de las instituciones públicas.
128	Definir marco e iniciar capacitaciones	Se propone elaborar un marco de gestión integral de riesgos de ciberseguridad a nivel nacional incorporando el enfoque de género con perspectiva interseccional para proteger los derechos de las personas dadas sus diversas necesidades, y ii) establecer procesos de seguimiento y revisión periódica a la implementación del marco de gestión integral de riesgos de ciberseguridad adaptándolo a las nuevas amenazas, vulnerabilidades y tendencias en el ámbito de la ciberseguridad
129	Definir servicios esenciales, activos críticos, y clasificación de la información.	Se propone i) definir y evaluar periódicamente los criterios para designar infraestructuras críticas nacionales teniendo en cuenta la protección de los derechos humanos de las personas dadas sus diversas necesidades, ii) identificar a los operadores que ejercen el control sobre las infraestructuras críticas nacionales y prestan servicios esenciales, y iii) identificar y categorizar las infraestructuras críticas nacionales
130	Desarrollar un plan de capacitación especializado para este principio permitiendo unificar criterios y formas de atención	Se propone elaborar y ejecutar programas de desarrollo de capacidades y habilidades de ciberseguridad para profesionales que ejercen la protección de infraestructuras críticas nacionales y en operadores de servicios esenciales
131	Divulgación de acciones a los ciudadanos	Se propone divulgar información oportuna y confiable sobre riesgos de ciberseguridad que afectan a la sociedad costarricense resaltando aquellos debidos al género y otras interseccionalidades.
132	El ser humano por lo general le pone crítico a todo y hay aspectos importantes más a nivel país hay elementos que son críticos. Debe existir un metodología clara, práctica y repetible para poder identificar esas estructuras críticas (evitando subjetividades) para que a partir de dicha identificación se puedan tomar decisiones y realizar una adecuada evaluación de riesgos	Se propone i) definir y evaluar periódicamente los criterios para designar infraestructuras críticas nacionales teniendo en cuenta la protección de los derechos humanos de las personas dadas sus diversas necesidades, ii) identificar a los operadores que ejercen el control sobre las infraestructuras críticas nacionales y prestan servicios esenciales, iii) identificar y categorizar las infraestructuras críticas nacionales, y iii) identificar y categorizar las infraestructuras críticas nacionales.
133	Es importante educar a nuestras instituciones sobre los grados de madurez que podemos tener en la resiliencia de un servicio y definir planes ajustados para proteger esas infraestructuras críticas con base en mejores prácticas y recursos asignados	Se propone i) definir y evaluar periódicamente los criterios para designar infraestructuras críticas nacionales teniendo en cuenta la protección de los derechos humanos de las personas dadas sus diversas necesidades, ii) identificar a los operadores que ejercen el control sobre las infraestructuras críticas nacionales y prestan servicios esenciales, iii) identificar y categorizar las infraestructuras críticas nacionales, y iii) identificar y categorizar las infraestructuras críticas nacionales.
134	Establecer los mecanismos de comunicación para la efectiva divulgación de información, monitoreo y detección temprana de posibles actividades sospechosas que puedan provocar un incidente, atención oportuna e implementación de las acciones necesarias para la corrección y protección de la infraestructura, evaluación de la situación y generación de documentación sobre lecciones aprendidas, retroalimentación, mejoras en procesos o procedimientos establecidos, mejora continua.	Se propone i) desarrollar estrategias, protocolos y mecanismos de comunicación que promuevan la participación de todas las múltiples partes interesadas, especialmente de la academia y sector privado y que rindan cuentas de la ejecución del plan de acción, y ii) divulgar información oportuna y confiable sobre riesgos de ciberseguridad que afectan a la sociedad costarricense resaltando aquellos debidos al género y otras interseccionalidades.
135	Establecer redes de intercambio de información e inteligencia, así como de buenas prácticas con unidades internacionales especializadas en la materia y Estados aliados.	Se propone i) promover la celebración de convenios y acuerdos de cooperación internacional bilaterales y/o multilaterales relevantes sobre ciberseguridad y lucha contra el ciberdelito, y ii) fortalecer la participación del CSIRT-CR en redes regionales e internacionales de equipos de respuesta a incidentes como la Red CSIRTS Américas de la OEA/CICTE.
136	Evaluar la idoneidad de los sistemas y proveedores de soluciones de ciberseguridad con los que se cuenta hasta el momento	Se propone adelantar evaluaciones de riesgos de ciberseguridad de las infraestructuras críticas nacionales en conjunto con los operadores de servicios esenciales.
137	Fortalecer la rectoría y seguimiento del MICITT para establecer lineamientos y caminos a seguir	Se propone crear y ejecutar un plan de fortalecimiento de capacidades operativas, administrativas, humanas, científicas y de infraestructura física y tecnológica del Centro de Respuesta de Incidentes de Seguridad Informática (CSIRT-CR) para consolidarlo como equipo de respuesta nacional a incidentes de ciberseguridad.
138	Identificar con claridad el pensar de los Sectores Financiero, Seguros, Telecomunicaciones, Universidades Estatales, Cooperativismo, Solidarismo y PYME. En los ejercicios debe poder identificarse su pensar dado el peso en la economía y el impacto que implica un evento en sus infraestructuras.	Se propone coordinar ejercicios y simulacros nacionales de ciberseguridad para probar el estado de preparación de los operadores de infraestructuras críticas nacionales y de servicios esenciales.
139	Identificar las personas de contacto y atención debida según la infraestructura que se determine como crítica	Se propone establecer mecanismos específicos de cooperación con operadores de infraestructuras críticas nacionales y operadores de servicios esenciales.
140	Identificar los requerimientos de RH requeridos en cada institución, independientemente de su prioridad, y MICITT como ente rector, velar porque se supla ese requerimiento.	Se propone formular e implementar una estrategia de desarrollo de fuerza laboral de ciberseguridad a nivel nacional atendiendo las necesidades del mercado laboral y las tendencias en ciberseguridad, así como promoviendo la diversidad, igualdad de género e inclusión social.

#	APORTE	CONSIDERACIONES
141	Integrar a todas las instituciones en un modelo de gestión de riesgos que consolide en un único proceso de análisis	Se propone elaborar un marco de gestión integral de riesgos de ciberseguridad a nivel nacional incorporando el enfoque de género con perspectiva interseccional para proteger los derechos de las personas dadas sus diversas necesidades.
142	La capacitación de todos los actores, en materia de TI, según su especialización, virtualización, Bases de Datos, redes, servidores, programadores etc.	Se propone mejorar y expandir las capacidades y habilidades cibernéticas en todos los niveles
143	La concientización a la población, generar desde las escuelas, colegios, institutos y universidades una educación y cultura de ciberseguridad siendo esta responsabilidad de todos. Realizar simulacros activos de ciber ataques	Se propone i) elaborar e implementar un plan nacional de educación y formación en ciberseguridad en todos los niveles del sistema educativo costarricense y promoviendo el fortalecimiento del currículo considerando contenidos de ciberseguridad y la diversidad, igualdad de género e inclusión social y ii) coordinar ejercicios y simulacros nacionales de ciberseguridad para probar el estado de preparación de los operadores de infraestructuras críticas nacionales y de servicios esenciales.
144	La intercomunicación entre instituciones, mediante reuniones multidisciplinarias en donde se toquen los temas relacionados y se compartan experiencias	Se propone diseñar y poner en marcha un marco de gobernanza nacional de ciberseguridad promoviendo la participación de las múltiples partes interesadas, incluyendo autoridades nacionales y organizaciones de sociedad civil que defienden derechos de las personas dadas sus diversas necesidades.
145	Lo primero es la concientización en las instituciones sobre la importancia de la ciberseguridad y que es fundamental cumplir con los parámetros mínimos al menos y por otro lado la constante revisión de las plataformas para en la medida de lo posible fortalecer el entorno completo. Desde el usuario final hasta la infraestructura crítica.	Se propone desarrollar campañas nacionales de concientización sobre la gestión integral de riesgos de ciberseguridad basándose en mejores prácticas dirigida a las múltiples partes interesadas con enfoque de género y con perspectiva interseccional.
146	Personal especializado, capacitación en treath hunter y presupuesto para compra de herramientas de seguridad o contratar servicios externos qué apoyen la prevención, contención y Resiliencia	Se propone i) desarrollar un plan de inversión que garantice la disponibilidad y asignación de recursos suficientes en instituciones públicas para llevar a cabo iniciativas de ciberseguridad, ii) promover en las instituciones públicas a contar con recursos financieros presupuestando anualmente aquellos necesarios para la gestión integral de riesgos de ciberseguridad, y iii) establecer procesos eficientes para la adquisición y compra de recursos tecnológicos en instituciones públicas para garantizar una gestión integral de los riesgos de ciberseguridad.
147	Prioridad 1, 2 y 3, antes de todo lo anterior son marcos de referencia y normativos ya adoptados y probados como el NIST e ISO27000, además de adherencia y cumplimiento estricto con normas de privacidad de la información como GDPR europeo que es la más estricta, que se tengan que seguir no solo a nivel público sino privado. Las directrices ya adoptadas a nivel ejecutivo en Estados Unidos deben ser aplicables en nuestro contexto siendo las anteriores normativas están establecidas y maduras, NO hace falta que inventen nada ni tropicalicen que lo único que harán es dar paso a brechas. El adherirse a normas establecidas por los países con quienes tenemos relación estrecha tendrán beneficios generales al país en términos de competitividad y seriedad internacional fundamentalmente.	Se propone i) actualizar el marco normativo para fortalecer los procesos de gestión administrativa y técnica del Centro de Respuesta de Incidentes de Seguridad Informática (CSIRT-CR), ii) establecer estándares, protocolos y procedimientos técnicos para la prevención, contención, resolución y respuesta a incidentes de ciberseguridad a nivel nacional, y iii) promover la celebración de convenios y acuerdos de cooperación internacional bilaterales y/o multilaterales relevantes sobre ciberseguridad y lucha contra el ciberdelito.
148	Priorizar la implementación de mejores prácticas utilizando estándares de la industria como CIS, NIST-CSF COBIT etc.	Se propone establecer estándares, protocolos y procedimientos técnicos para la prevención, contención, resolución y respuesta a incidentes de ciberseguridad a nivel nacional,
149	Procurar que la mayor parte de instituciones públicas cuenten con las mismas herramientas de defensa y SOC para que la atención de los incidentes sea más versátil a nivel nacional	Se propone i) establecer procesos eficientes para la adquisición y compra de recursos tecnológicos en instituciones públicas para garantizar una gestión integral de los riesgos de ciberseguridad., y ii) implementar sistemas avanzados de alerta y respuesta intersectorial ante incidentes de ciberseguridad en instituciones públicas.
150	Que el Gobierno de turno respete los esfuerzos realizados en estos talleres, así como aspectos legalidad relacionados a la ciberseguridad	Se propone una visión cohesiva y convincente construida con todas las múltiples partes interesadas, incluidos los sectores público y privado, las organizaciones de la sociedad civil, la academia y la comunidad en general, abordando las necesidades y los desafíos únicos de la ciudadanía costarricense, promoviendo la igualdad de oportunidades y la participación inclusiva en las iniciativas de ciberseguridad
151	Reconocer que vamos a terminar con media docena de SOCs, si no más. Comunicaciones son claves.	Se propone i) crear y ejecutar una estrategia para promover la creación y el fortalecimiento de SOC sectoriales. y ii) desarrollar estrategias, protocolos y mecanismos de comunicación que promuevan la participación de todas las múltiples partes interesadas, especialmente de la academia y sector privado y que rindan cuentas de la ejecución del plan de acción.
152	Recursos	Se propone asignar eficientemente los recursos para la implementación de iniciativas de ciberseguridad
153	Reforzar todo esto con una ley que destine presupuesto para todos los procesos relacionados con Ciberseguridad y partidas para capacitación a su personal	Se propone i) asignar eficientemente los recursos para la implementación de iniciativas de ciberseguridad, y ii) apoyar a la Asamblea Legislativa en el trámite de iniciativas o proyectos para adecuar, adaptar y/o armonizar el marco legal relacionado con la ciberseguridad.
154	Capacitación	Se propone mejorar y expandir las capacidades y habilidades cibernéticas en todos los niveles en el país

#	APORTE	CONSIDERACIONES
155	Se debe considerar un proceso de gestión de riesgos más allá de los riesgos de Ciberseguridad o Seguridad de la Información, esto debe ser integral	Se propone elaborar un marco de gestión integral de riesgos de ciberseguridad a nivel nacional incorporando el enfoque de género con perspectiva interseccional para proteger los derechos de las personas dadas sus diversas necesidades.
156	Sensibilizar la población	Se propone desarrollar campañas nacionales de concientización sobre la gestión integral de riesgos de ciberseguridad basándose en mejores prácticas dirigida a las múltiples partes interesadas con enfoque de género y con perspectiva interseccional.
157	Si más del 25% de malos eventos de ciberseguridad se dan por errores humanos. Se debería de trabajar en pro de la educación y la concientización constante.	Se propone i) mejorar y expandir las capacidades y habilidades cibernéticas en todos los niveles en el país y ii) fomentar una cultura ciudadana responsable en ciberseguridad
158	Tener un mapa claro de cuál es la infraestructura con más riesgo	Se propone adelantar evaluaciones de riesgos de ciberseguridad de las infraestructuras críticas nacionales en conjunto con los operadores de servicios esenciales.
159	Todo abarca muy bien el tema	-
160	Capacitación rígida y periódica a los jerarcas de toma de decisiones, que por su desconocimiento bloquean acciones de suma importancia en el tema	Se propone elaborar y ejecutar programas de desarrollo de capacidades y habilidades de ciberseguridad para profesionales y altas y altos jerarcas en instituciones públicas.

Pilar 4. Educación, capacitación y concientización

Reforzar las capacidades del ecosistema de ciberseguridad, educando, capacitando, formando y concientizando a todas las múltiples partes interesadas y promoviendo la investigación y desarrollo de ciberseguridad

Líneas de Acción:

- Mejorar y expandir las capacidades y habilidades cibernéticas en todos los niveles con enfoque centrado en el ser humano y de género con perspectiva interseccional
- Fomentar una cultura ciudadana responsable en ciberseguridad
- Promover la investigación, el desarrollo y la innovación

A continuación, se presenta la valoración de las múltiples partes interesadas respecto de la importancia de las acciones propuestas para reforzar las capacidades del ecosistema de ciberseguridad en el país, resaltando que han sido catalogadas como urgentes y necesarias.

OBJETIVO ESTRATEGICO	#	LINEA DE ACCIÓN	#	#	INTERVENCIÓN PÚBLICA	Urgente	Necesaria	Postergable	Innecesaria	Total	Urgente	Necesaria	Postergable	Innecesaria	Total
Reforzar las capacidades del ecosistema de ciberseguridad	4.1	Mejorar y expandir las capacidades y habilidades cibernéticas en todos los niveles con enfoque centrado en el ser humano y de género con perspectiva interseccional	44	4.1.1	Plan nacional de educación y formación en ciberseguridad	45	14	1		60	75%	23%	2%	0%	100%
			45	4.1.2	Estrategia nacional de desarrollo de fuerza laboral de ciberseguridad	40	17	3		60	67%	28%	5%	0%	100%
			46	4.1.3	Programas de capacitación a sector público	47	12	1		60	78%	20%	2%	0%	100%
			47	4.1.4	Programas de capacitación a sector privado	22	31	7		60	37%	52%	12%	0%	100%
			48	4.1.5	Programas de capacitación a infraestructuras críticas nacionales	48	9	3		60	80%	15%	5%	0%	100%
			49	4.1.6	Programas de capacitación al sector de aplicación de la ley	33	23	4		60	55%	38%	7%	0%	100%
			50	4.1.7	Programas de capacitación a la ciudadanía	28	25	6	1	60	47%	42%	10%	2%	100%
	4.2	Fomentar una cultura ciudadana responsable en ciberseguridad	51	4.2.1	Campañas nacionales de concientización	37	21	2		60	62%	35%	3%	0%	100%
			52	4.2.2	Herramientas y recursos en línea de concientización	24	34	2		60	40%	57%	3%	0%	100%
			53	4.2.3	programa de concientización sobre ciberhigiene y uso responsable de tecnologías	35	24	1		60	58%	40%	2%	0%	100%
			54	4.2.4	Mecanismos de divulgación sobre estado de cibercrímen	30	25	4	1	60	50%	42%	7%	2%	100%
	4.3	Promover la investigación, el desarrollo y la innovación	55	4.3.1	Programa para impulsar la innovación y el desarrollo tecnológico	27	27	6		60	45%	45%	10%	0%	100%
			56	4.3.2	Estudios de investigación en el desarrollo y adopción segura de nuevas tecnologías emergentes y disruptivas	22	32	6		60	37%	53%	10%	0%	100%
			57	4.3.3	Plan de fomento a la creación de nuevas empresas	14	28	14	4	60	23%	47%	23%	7%	100%
			58	4.3.4	Estudios para promover investigación y desarrollo	18	22	17	3	60	30%	37%	28%	5%	100%

Nota: 60 respuestas

A continuación, se analizan los aportes de los participantes en las mesas presenciales en relación con las capacidades del ecosistema de ciberseguridad en el país.

#	APORTES	CONSIDERACIONES
161	1-Todas las capacitaciones, formaciones y concienciación deben estar alineadas a la estrategia Nacional de Ciberseguridad y enfocadas a todos los sectores de la sociedad.	Se propone desarrollar una fuerza laboral capacitada en ciberseguridad a través de programas de educación, capacitación y formación, promoverá la conciencia de ciberseguridad entre el público y fomentará una cultura de comportamiento en línea responsable y seguro.
162	A nivel país es necesario arrancar ya con una campaña general de concientización enfocada en los niveles de conocimiento, pero si abarcando desde una generalidad la importancia del tema	Se propone desarrollar campañas nacionales de concientización sobre la gestión integral de riesgos de ciberseguridad basándose en mejores prácticas dirigida a las múltiples partes interesadas con enfoque de género y con perspectiva interseccional.
163	Analizar la parte salarial de sector informático en las instituciones públicas.	Se propone formular e implementar una estrategia de desarrollo de fuerza laboral de ciberseguridad a nivel nacional
164	Aplicación de estándares mundiales para medir la capacidad de los profesionales que laboran en el área	Se propone i) establecer mecanismos de seguimiento y control de indicadores clave de rendimiento y de gestión integral de riesgos de ciberseguridad incluyendo indicadores que contribuyan a medir el impacto de género con perspectiva interseccional, y ii) adelantar evaluaciones de impacto socio económico respecto de la implementación de la Estrategia Nacional de Ciberseguridad 2023-2027.
165	Apoyarse en la Academia o la experiencia del INA	Se propone elaborar e implementar un plan nacional de educación y formación en ciberseguridad en todos los niveles del sistema educativo costarricense y promoviendo el fortalecimiento del currículo considerando contenidos de ciberseguridad y la diversidad, igualdad de género e inclusión social.
166	Apoyo en la creación e implementación de materiales de cultura digital para todos los sectores, incluyendo la población en general	Se propone desarrollar herramientas y recursos en línea, como tutoriales, videos y guías, que permitan a la ciudadanía costarricense adquirir y fortalecer habilidades en ciberseguridad.
167	Asegurar que el recurso humano con que cuenta una institución pueda mantenerse y que atienda temas de Ciberseguridad, eso sí dotándolo de la plaza/puesto apto/a para cumplir tal fin.	Se propone formular e implementar una estrategia de desarrollo de fuerza laboral de ciberseguridad a nivel nacional
168	Básicamente esas.	-
169	Capacidad de interactuar con otras instituciones	Se propone promover la celebración de iniciativas de cooperación, colaboración y asistencia intergubernamental e intersectorial.
170	Capacitación y presupuesto	Se propone i) mejorar y expandir las capacidades y habilidades cibernéticas en todos los niveles en el país y ii) asignar eficientemente los recursos para la implementación de iniciativas de ciberseguridad
171	Capacitación en Gestión de Riesgos	Se propone impulsar el cumplimiento del marco normativo técnico relacionado con la gestión integral de riesgos de ciberseguridad.
172	Capacitaciones urgentes en temas de normativas vigentes qué abordan las mejores prácticas de ciberseguridad tales como ISOS, NIST, COBIT, cursos sobre CISO, ETIKAL HAKING, etc.	Se propone elaborar y ejecutar programas de desarrollo de capacidades y habilidades de ciberseguridad para profesionales

#	APORTES	CONSIDERACIONES
		que ejercen la protección de infraestructuras críticas nacionales y en operadores de servicios esenciales
173	Como parte de la estrategia con efecto a corto y mediano plazo: Modificar e incluir en el tronco común de los programas de estudio de las carreras de informática, la materia de ciberseguridad y seguridad de la información.	Se propone elaborar e implementar un plan nacional de educación y formación en ciberseguridad en todos los niveles del sistema educativo costarricense y promoviendo el fortalecimiento del currículo considerando contenidos de ciberseguridad y la diversidad, igualdad de género e inclusión social.
174	Concientización a los jerarcas de las diferentes instituciones y ministerios sobre la importancia de la seguridad informática y el cumplimiento de normas de ciberseguridad, con el finde recibir el apoyo necesario para ejecutar un plan de acción a nivel nacional.	Se propone elaborar y ejecutar programas de desarrollo de capacidades y habilidades de ciberseguridad para profesionales y altas y altos jerarcas en instituciones públicas.
175	Crear planes de simulacros de ataques	Se propone coordinar ejercicios y simulacros nacionales de ciberseguridad para probar el estado de preparación de los operadores de infraestructuras críticas nacionales y de servicios esenciales.
176	Deberían aprovechar los CSIRT del MICITT para implementar a la sociedad educación en ciberseguridad	Se propone elaborar e implementar un plan nacional de educación y formación en ciberseguridad en todos los niveles del sistema educativo costarricense y promoviendo el fortalecimiento del currículo considerando contenidos de ciberseguridad y la diversidad, igualdad de género e inclusión social.
177	Divulgación de políticas y consejos de mejores prácticas enfocadas a pymes y emprendedores	Se propone elaborar y ejecutar programas de desarrollo de capacidades y habilidades de ciberseguridad para profesionales y altos directivos en organizaciones privadas, haciendo énfasis en MIPYMES.
178	Elaborar y ejecutar programas de desarrollo de capacidades y habilidades de ciberseguridad para las MIPYMES.	Se propone elaborar y ejecutar programas de desarrollo de capacidades y habilidades de ciberseguridad para profesionales y altos directivos en organizaciones privadas, haciendo énfasis en MIPYMES.
179	Estandarizar la información para cada uno de los sectores	Se propone establecer mecanismos eficientes asegurando el correcto procesamiento, administración, almacenamiento, compartición e intercambio de información sobre incidentes de ciberseguridad entre las múltiples partes interesadas incluyendo la aplicación de estándares recomendados por la industria y la participación en redes regionales e internacionales como la Red CSIRT Américas de la OEA/CICTE.
180	Financiamiento y capacitación para sociedad civil	Se propone i) mejorar y expandir las capacidades y habilidades cibernéticas en todos los niveles en el país y ii) asignar eficientemente los recursos para la implementación de iniciativas de ciberseguridad
181	Fomentar la Investigación y Desarrollo en Ciberseguridad: Invertir en investigación y desarrollo en ciberseguridad a nivel nacional para impulsar la innovación y el desarrollo de soluciones avanzadas de ciberseguridad.	Se propone establecer un programa para impulsar la innovación y el desarrollo tecnológico intersectorial en ciberseguridad especialmente en el ámbito de la protección y resiliencia de infraestructuras críticas nacionales.
182	Fomentar que las campañas lleguen también a las comunidades y zonas rurales. Actualmente se concentran en la GAM	Se propone diseñar y poner en marcha un marco de gobernanza nacional de ciberseguridad promoviendo la participación de las múltiples partes interesadas, incluyendo autoridades nacionales y organizaciones de sociedad civil que defienden derechos de las personas dadas sus diversas necesidades.
183	Formación de recurso humano es la clave.	Se propone desarrollar una fuerza laboral capacitada en ciberseguridad a través de programas de educación, capacitación y formación, promover la conciencia de ciberseguridad entre el público y fomentar una cultura de comportamiento en línea responsable y seguro.
184	Hacer énfasis en fortalecer en conocimientos a la sociedad, empresas, instituciones etc. en una cultura de educación, desarrollo y buenas prácticas a nivel de Ciberseguridad como una tarea cotidiana.	Se propone elaborar e implementar un plan nacional de educación y formación en ciberseguridad en todos los niveles del sistema educativo costarricense y promoviendo el fortalecimiento del currículo considerando contenidos de ciberseguridad y la diversidad, igualdad de género e inclusión social.
185	Hay que aprovechar iniciativas que se tengan a nivel nacional de los diferentes sectores para promover una mayor colaboración. Toda estrategia de concientización debe considerar los diferentes grupos de la población para que los mensajes sean efectivos con casos prácticos en un lenguaje de fácil comprensión	Se propone desarrollar campañas nacionales de concientización sobre la gestión integral de riesgos de ciberseguridad basándose en mejores prácticas dirigida a las múltiples partes interesadas con enfoque de género y con perspectiva interseccional.
186	Idear un plan de capacidades y posterior a esto, proponer una Estructura profesional mínima en ciberseguridad que deben tener las instituciones basado en su naturaleza, presupuesto y funciones críticas.	Se propone formular e implementar una estrategia de desarrollo de fuerza laboral de ciberseguridad a nivel nacional atendiendo las necesidades del mercado laboral y las tendencias en ciberseguridad, así como promoviendo la diversidad, igualdad de género e inclusión social.
187	Identificar necesidades de formación por grupos etarios, cubriendo a toda la población	Se propone formular e implementar una estrategia de desarrollo de fuerza laboral de ciberseguridad a nivel nacional atendiendo las necesidades del mercado laboral y las tendencias en ciberseguridad, así como promoviendo la diversidad, igualdad de género e inclusión social.
188	Implementación de marco como 27001, NIST	Se propone establecer estándares, protocolos y procedimientos técnicos para la prevención, contención, resolución y respuesta a incidentes de ciberseguridad a nivel nacional

#	APORTES	CONSIDERACIONES
189	Implementar ciberseguridad como parte de los estudios generales en universidad pública y privada	Se propone elaborar e implementar un plan nacional de educación y formación en ciberseguridad en todos los niveles del sistema educativo costarricense y promoviendo el fortalecimiento del currículo considerando contenidos de ciberseguridad y la diversidad, igualdad de género e inclusión social.
190	Implementar un modelo de verificación d de la calidad de la formación qué se brindan en instituciones o entidades sobre ciberseguridad	Se propone formular e implementar una estrategia de desarrollo de fuerza laboral de ciberseguridad a nivel nacional atendiendo las necesidades del mercado laboral y las tendencias en ciberseguridad, así como promoviendo la diversidad, igualdad de género e inclusión social.
191	Incluir perspectiva de género y derechos humanos.	Se propone una estrategia con perspectiva de género bajo enfoque de Derechos Humanos y Enfoque centrado en el ser humano con principios rectores como el respeto a los Derechos Humanos y los valores fundamentales.
192	La ciberseguridad, no tiene género, ni edad... los ciberdelincuentes no se fijan en estos temas...	Se propone una estrategia con visión cohesiva y convincente construida con todas las múltiples partes interesadas, incluidos los sectores público y privado, las organizaciones de la sociedad civil, la academia y la comunidad en general, abordando las necesidades y los desafíos únicos de la ciudadanía costarricense, promoviendo la igualdad de oportunidades y la participación inclusiva en las iniciativas de ciberseguridad
193	La educación de la sociedad en el tema de la Ciberseguridad, mejores prácticas, controles parentales, filtración de programación y temáticas en el entorno familiar.	Se propone crear un programa de concientización en prácticas de ciber higiene y uso responsable de la tecnología para la población en general, y para las infancias y adolescencias en particular.
194	La capacitación general a personal de gobierno y empresas privadas permitirá unificar criterios y conocimientos.	Se propone i) elaborar y ejecutar programas de desarrollo de capacidades y habilidades de ciberseguridad para profesionales y altas y altos jerarcas en instituciones públicas, y ii) elaborar y ejecutar programas de desarrollo de capacidades y habilidades de ciberseguridad para profesionales y altos directivos en organizaciones privadas, haciendo énfasis en MIPYMES.
195	La transformación cultural de la sociedad en una sociedad digital lo que lleva intrínseco ese conocimiento de temas de ciberseguridad	Se propone fomentar una cultura ciudadana responsable en ciberseguridad
196	Lograr un axioma de las propuestas anteriores y que se genere una alianza privada con el MEP para preparar el recurso humano de forma tal que vayan desarrollando nuevas capacidades desde la educación básica y puedan integrarse en perfiles técnicos recién graduados de la educación formal con la posibilidad de continuar carreras tecnológicas una vez que laboran	Se propone elaborar e implementar un plan nacional de educación y formación en ciberseguridad en todos los niveles del sistema educativo costarricense y promoviendo el fortalecimiento del currículo considerando contenidos de ciberseguridad y la diversidad, igualdad de género e inclusión social.
197	Mantenerse en constante comunicación con la ciudadanía, pensando en las personas que son 0 tecnología.	Se propone elaborar y ejecutar programas de desarrollo de capacidades y habilidades de ciberseguridad para la sociedad costarricense en general reconociendo las necesidades de seguridad diferenciadas e interseccionales de las personas y comunidades.
198	Modificar el programa de educación para ingresar como punto la seguridad de los datos	Se propone elaborar e implementar un plan nacional de educación y formación en ciberseguridad en todos los niveles del sistema educativo costarricense y promoviendo el fortalecimiento del currículo considerando contenidos de ciberseguridad y la diversidad, igualdad de género e inclusión social.
199	Muchas de las acciones propuestas no son de elaboración sino de coordinación. Es importante revisar qué existe en estos temas desde todos los sectores para no dispersar esfuerzos.	Se propone i) diseñar y poner en marcha un marco de gobernanza nacional de ciberseguridad promoviendo la participación de las múltiples partes interesadas, incluyendo autoridades nacionales y organizaciones de sociedad civil que defienden derechos de las personas dadas sus diversas necesidades, y ii) crear y poner en marcha mecanismos dinámicos de coordinación, y colaboración e intercambio de información intergubernamental e intersectorial vinculando a las múltiples partes interesadas.
200	Ninguna más por el momento	-
201	No estoy de acuerdo con promover la publicación del estado del cibercrimen a la población ya que esto pondría en alerta a los cibercriminales y podría atraer a nuevos actores de amenazas. Los estudios de investigación en el desarrollo y adopción segura de nuevas tecnologías emergentes y disruptivas deben hacerse desde la academia en conjunto con MICITT e Inteligencia. La creación de nuevas empresas, en alianza con incubadoras y aceleradoras de emprendimiento debe ir de la mano con la formación de profesionales en distintos niveles.	Se propone elaborar estudios de investigación en el desarrollo y adopción segura de nuevas tecnologías emergentes y disruptivas junto con su impacto en la ciberseguridad.
202	No solo elaborar los programas, buscar la forma del cómo implementarlos	Se propone establecer e implementar un programa para impulsar la innovación y el desarrollo tecnológico intersectorial en ciberseguridad especialmente en el ámbito de la protección y resiliencia de infraestructuras críticas nacionales.
203	Plan Ciberseguridad alineada a políticas nacionales que garanticen su aplicabilidad y evaluar los recursos que se cuentan	Se propone i) mejorar y expandir las capacidades y habilidades cibernéticas en todos los niveles en el país y ii) asignar eficientemente los recursos para la implementación de iniciativas de ciberseguridad
204	Capacitación	Se propone mejorar y expandir las capacidades y habilidades cibernéticas en todos los niveles en el país

#	APORTES	CONSIDERACIONES
205	Primero enfocaría los esfuerzos en diagnosticar qué se requiere y en dónde y priorizar los contenidos y esfuerzos allí primero	Se propone
206	Promover el intercambio de buenas prácticas y experiencias con otros estados	Se propone promover la celebración de convenios y acuerdos de cooperación internacional bilaterales y/o multilaterales relevantes sobre ciberseguridad y lucha contra el ciberdelito.
207	Promover las alianzas público-privadas en coordinación para lograr juntos la meta en común: un fuerte ante el cibercrimen, país competente y líder en ciberseguridad	Se propone fortalecer las alianzas del sector público con el sector privado, las organizaciones de la sociedad civil y la academia.
208	Recursos	Se propone asignar eficientemente los recursos para la implementación de iniciativas de ciberseguridad
209	Reforzar la concientización a todo nivel.	Se propone desarrollar campañas nacionales de concientización sobre la gestión integral de riesgos de ciberseguridad basándose en mejores prácticas dirigida a las múltiples partes interesadas con enfoque de género y con perspectiva interseccional.
210	Sensibilizar y curar contenido según poblaciones. Informar para minimizar riesgos y maximizar oportunidades sin crear pánico moral ni deshumanización. Programas no formales son importantes que apuesten por algo más allá a lo curricular.	Se propone elaborar e implementar un plan nacional de educación y formación en ciberseguridad en todos los niveles del sistema educativo costarricense y promoviendo el fortalecimiento del currículo considerando contenidos de ciberseguridad y la diversidad, igualdad de género e inclusión social.
211	Todas las anteriores	-
213	Todo considerado	-

Pilar 5. Cooperación y alianzas

Cooperar en el entorno digital, construyendo alianzas público-privadas y ejerciendo ciber diplomacia en pro de un orden internacional más seguro, próspero y abierto.

Líneas de Acción:

- Fortalecer la cooperación, colaboración y asistencia en ciberseguridad entre las múltiples partes interesadas a nivel nacional
- Maximizar los beneficios de la cooperación cibernética internacional

A continuación, se presenta la valoración de las múltiples partes interesadas respecto de la importancia de las acciones propuestas para cooperar en el entorno digital del país, resaltando que han sido catalogadas como urgentes y necesarias.

OBJETIVO ESTRATEGICO	#	LINEA DE ACCIÓN	#	#	INTERVENCIÓN PÚBLICA	Urgente	Necesaria	Postergable	Innecesaria	Total	Urgente	Necesaria	Postergable	Innecesaria	Total
Cooperar en el entorno digital	5.1	Fortalecer la cooperación, colaboración y asistencia en ciberseguridad entre las múltiples partes interesadas a nivel nacional	59	5.1.1	Iniciativas de cooperación, colaboración y asistencia intergubernamental e intersectorial	15	31	1	1	48	31%	65%	2%	2%	100%
			60	5.1.2	Alianzas con sector privado, organizaciones de la sociedad civil y academia	27	21			48	56%	44%	0%	0%	100%
			61	5.1.3	Mecanismos de cooperación con operadores de infraestructuras críticas nacionales	33	14	1		48	69%	29%	2%	0%	100%
	5.2	Maximizar los beneficios de la cooperación cibernética internacional	62	5.2.1	Responsable de ciber diplomacia	11	27	7	3	48	23%	56%	15%	6%	100%
			63	5.2.2	Convenios y acuerdos de cooperación internacional bilaterales y/o multilaterales	17	28	2	1	48	35%	58%	4%	2%	100%
			64	5.2.3	Fortalecimiento de la participación del CSIRT-CR en redes internacionales	30	18			48	63%	38%	0%	0%	100%
			65	5.2.4	Alianzas con instituciones de otras ramas del poder público en torno a la cooperación internacional	15	30	3		48	31%	63%	6%	0%	100%
			66	5.2.5	Mecanismos de cooperación con organismos de seguridad y justicia internacionales	31	17			48	65%	35%	0%	0%	100%
			67	5.2.6	Participación del país en operaciones internacionales	20	23	5		48	42%	48%	10%	0%	100%
			68	5.2.7	Participación del país en discusión y desarrollo de normativas internacionales	17	29	2		48	35%	60%	4%	0%	100%
			69	5.2.8	Participación del país sobre comportamiento responsable de los Estados e implementación Res UN 1325	11	31	6		48	23%	65%	13%	0%	100%

Nota: 48 respuestas

A continuación, se analizan los aportes de los participantes en las mesas presenciales en relación con la cooperación en el entorno digital del país.

#	APORTES	CONSIDERACIONES
214	1-Cooperación intersectorial. 2-Incluir el tema de sostenibilidad del modelo y servicios	Se propone impulsar la cooperación nacional e internacional, la colaboración y el intercambio de información sobre cuestiones de ciberseguridad
215	Acompañamiento y asistencia de las instituciones u organizaciones con menos desarrollo, información y capacidades a niveles de Ciberseguridad.	Se propone promover la celebración de iniciativas de cooperación, colaboración y asistencia intergubernamental e intersectorial.
216	Agregar a los currículos o programas de estudio en escuelas colegios y universidades formación obligatoria en ciberseguridad	Se propone elaborar e implementar un plan nacional de educación y formación en ciberseguridad en todos los niveles del sistema educativo costarricense y promoviendo el fortalecimiento del currículo considerando contenidos de ciberseguridad y la diversidad, igualdad de género e inclusión social.
217	Apoyar la creación de leyes y normativas que fortalezcan el entorno jurídico digital del país.	Se propone desarrollar legislación y regulación cibernética junto con un marco normativo técnico para la ciberseguridad
218	Básicamente esas.	-
219	Cero politiquerías	-
220	Cooperación entre países	Se propone promover la celebración de convenios y acuerdos de cooperación internacional bilaterales y/o multilaterales relevantes sobre ciberseguridad y lucha contra el ciberdelito.
221	Cooperación y capacitación	Se propone promover la celebración de iniciativas de cooperación, colaboración y asistencia intergubernamental e intersectorial.
222	Cooperación y capacitación internacional.	Se propone promover la celebración de iniciativas de cooperación, colaboración y asistencia intergubernamental e intersectorial.
223	Dar fortaleza al MICITT y que no se algo político que cambie cada 4 años y se pierda los esfuerzos.	Se propone fortalecer la instancia de coordinación nacional para dirigir la implementación de la Estrategia Nacional de Ciberseguridad 2023-2027 y hacer seguimiento continuo, dotándola de herramientas jurídicas y técnicas que le permitan desempeñar sus funciones con la mayor efectividad
224	Definir una unidad de ciber diplomacia a lo interno del Ministerio de Relaciones Exteriores y Culto a cargo de la cooperación internacional.	Se propone nombrar responsabilidades organizativas para asuntos exteriores cibernéticos (embajador cibernético u otra oficina dedicada) e informar regularmente sobre la cooperación internacional a nivel político / estratégico.
225	El CNTD habla sobre la interoperabilidad es importante a nivel ciberseguridad establecer un estándar básico, siempre teniendo en cuenta presupuesto, infraestructura de las MiPymes y pequeña a mediana empresa. Esto por las diferentes particularidades de cada empresa del país y estas también a su vez al lograr ligarse, cooperen con las demás logrando así tener una red de apoyo y cooperación nacional.	Se propone establecer estándares, protocolos y procedimientos técnicos para la prevención, contención, resolución y respuesta a incidentes de ciberseguridad a nivel nacional
226	Es necesario la ayuda internacional para tomar modelos exitosos en otros países en la educación desde un ciber higiene digital o ciberseguridad para mejorar el conocimiento de todos los estratos de la población	Se propone participar en la discusión y desarrollo de normativas internacionales que aborden los desafíos de ciberseguridad y promuevan un ciberespacio estable, seguro y confiable comprendiendo el impacto de las operaciones cibernéticas maliciosas en los grupos vulnerables.
227	Establecer foros de Transferencia de conocimiento entre personal dedicado a labores de ciberseguridad con respecto a prevención, control y mitigación relacionados a ciberseguridad	Se propone desarrollar una fuerza laboral capacitada en ciberseguridad a través de programas de educación, capacitación y formación, promover la conciencia de

#	APORTES	CONSIDERACIONES
		ciberseguridad entre el público y fomentar una cultura de comportamiento en línea responsable y seguro
228	Establecer las estructuras, los entes, responsables y enlaces para aprovechar la cooperación internacional, que colabore con el conocimiento, competencias y estrategias para el crecimiento del Sistema de Apoyo a la Ciberseguridad.	Se propone diseñar y poner en marcha un marco de gobernanza nacional de ciberseguridad promoviendo la participación de las múltiples partes interesadas, incluyendo autoridades nacionales y organizaciones de sociedad civil que defienden derechos de las personas dadas sus diversas necesidades.
229	Establecer un órgano conjunto MICITT DIS Cancillería para coordinar los asuntos de ciber diplomacia que aborden temas de ciberseguridad nacional	Se propone nombrar responsabilidades organizativas para asuntos exteriores cibernéticos (embajador cibernético u otra oficina dedicada) e informar regularmente sobre la cooperación internacional a nivel político / estratégico.
230	Esto es materia de Relaciones Exteriores en coordinación con MIDEPLAN	Se propone promover la celebración de iniciativas de cooperación, colaboración y asistencia intergubernamental e intersectorial.
231	"Fundamental fortalecer las alianzas (cooperación, ayuda, capacitación, etc.) entre instituciones a nivel nacional "	Se propone fortalecer la cooperación, colaboración y asistencia en ciberseguridad entre las múltiples partes interesadas a nivel nacional
232	Habilitar fondos para la investigación de patrones, casos y resolución de problemas para analizar, inventariar y divulgar.	Se propone asignar eficientemente los recursos para la implementación de iniciativas de ciberseguridad
233	Importante es que está cooperación pueda articularse entre diferentes organismos reforzadores del orden público para analizar en conjunto con el MICITT hacia donde está apuntando la información de inteligencia y prepararse muy de previo a posibles ataques	Se propone promover alianzas con instituciones de otras ramas del poder público, en especial con aquellas instancias que rigen como autoridad central o puntos de contacto en el país para diversos convenios y tratados de cooperación internacional en materia de ciberseguridad y de lucha contra la ciberdelincuencia.
234	La cooperación es primordial en la Ciberseguridad, debemos trabajar unidos y en equipo.	Se propone promover la celebración de iniciativas de cooperación, colaboración y asistencia intergubernamental e intersectorial.
235	Monitoreo, seguimiento y reforzar capacidades para sociedad civil	Se propone elaborar y ejecutar programas de desarrollo de capacidades y habilidades de ciberseguridad para la sociedad costarricense en general reconociendo las necesidades de seguridad diferenciadas e interseccionales de las personas y comunidades.
236	Para muchas de estas acciones es urgente e impostergable la incorporación del Poder Judicial en la gobernanza de la estrategia. Importante tener en cuenta que la base para la cooperación es la confianza y esta debe construirse a su vez sobre las bases de la transparencia y el respeto entre sectores.	Se propone diseñar y poner en marcha un marco de gobernanza nacional de ciberseguridad promoviendo la participación de las múltiples partes interesadas (incluyendo Poder Judicial), incluyendo autoridades nacionales y organizaciones de sociedad civil que defienden derechos de las personas dadas sus diversas necesidades.
237	Promover que mediante los programas de responsabilidad social de las grandes corporaciones se generen espacios de transferencia de experiencias y capacitación a nivel país	Se propone formular e implementar una estrategia de desarrollo de fuerza laboral de ciberseguridad a nivel nacional atendiendo las necesidades del mercado laboral y las tendencias en ciberseguridad, así como promoviendo la diversidad, igualdad de género e inclusión social.
238	Recursos	Se propone asignar eficientemente los recursos para la implementación de iniciativas de ciberseguridad
239	Se requieren alianzas nacionales e internacionales con el fin de potenciar el objetivo común de la ciberseguridad	Se propone promover la celebración de iniciativas de cooperación, colaboración y asistencia intergubernamental e intersectorial.
240	Se ven los puntos importantes, se puede usar el tratado de Budapest como donante a nuestro país	Se propone participar en la discusión y desarrollo de normativas internacionales que aborden los desafíos de ciberseguridad y promuevan un ciberespacio estable, seguro y confiable comprendiendo el impacto de las operaciones cibernéticas maliciosas en los grupos vulnerables.
241	Todas las alianzas que se establezcan generen protocolos, guías, estándares que promuevan dar pasos en una hoja de ruta o madurez en seguridad	Se propone fortalecer las alianzas del sector público con el sector privado, las organizaciones de la sociedad civil y la academia.
242	Todas las anteriores	-
243	Todo ok	-
244	Trabajo en conjunto con el sector privado tanto en capacitaciones como soluciones relacionadas a ciberseguridad con el fin de colaborar mutuamente en el desarrollo de las fuerzas técnicas	Se propone fortalecer las alianzas del sector público con el sector privado, las organizaciones de la sociedad civil y la academia.

Aportes de las partes interesadas en las mesas de trabajo virtuales

#	APORTES
1	Que los jerarcas participen más activamente en la estrategia, así como se requiere más contenido presupuestario para poder llevar adelante la tarea
2	Brindar recursos tanto económicos como de personal, además de capacitación
3	Plataforma interministerial
10	Mejorar Presupuesto, plazas, salario ya que posterior de conocimiento se prestaría con fuga de personal con conocimiento, especialidad en ciberseguridad
11	Considero que en virtud de que en todas las instituciones los recursos son escasos, se podría valorar que la estrategia de ciberseguridad incluya una directriz relacionada con la inversión en la ciberseguridad de tal manera que se establezca un porcentaje mínimo de inversión del total del presupuesto de cada institución, dedicada a las acciones de ciberseguridad.
12	Debemos hacer un plan integrado nivel país y estandarizar los sistemas. Ya que, si se integran todas las instituciones públicas, se podría trabajar en tiempo real. A nivel urgente es tratar de concientizar a los altos jerarcas para brindar presupuesto. En mi caso, yo me pague el Técnico en Ciberseguridad, porque no se puede esperar que todo nos lo den en la mano, tenemos que poner nuestro grano de arena.
13	Grupo de apoyo interinstitucional capacitado en ciber y evitar la fuga con el fin de la continuidad del servicio.
14	Debemos hacer un plan integrado nivel país y estandarizar los sistemas. Ya que, si se integran todas las instituciones públicas, se podría trabajar en tiempo real. A nivel urgente es tratar de concientizar a los altos jerarcas para brindar presupuesto. En mi caso, yo me pague el Técnico en Ciberseguridad, porque no se puede esperar que todo nos lo den en la mano, tenemos que poner nuestro grano de arena.
15	Un plan de capacitación permanente para usuarios finales y personal de TI Más personal para atender las necesidades Reuniones trimestrales para estar al tanto de las acciones del CSIRT y el NOC Apoyo interinstitucional para atender necesidades de apoyo en temas de Ciber
16	Importante no generalizar a la hora de pedir tiempos de respuesta por ejemplo para capacitar o hacer alguna acción preventiva, ya que hay entidades pequeñas, medianas y grandes, desde entidades de menos de 100 funcionarios, otras de 1000 y otras con mas 50000 funcionarios
17	Si bien la ciberseguridad podría llevar una línea similar para cualquier Ministerio o empresa, la diferencia entre los ministerios en la cantidad de personal especializado y la estructura organizacional que tiene la unidad administrativa. En MIVAH somos solo 7 personas para cubrir todo: además de lo que se atiende relacionado a TI, se deben cubrir muchos otros aspectos y responsabilidades como desarrollos, gestión de proveedores e infraestructura, mantenimiento de sistemas, soporte técnico, atención a usuarios, gestión de proyectos, gestión de compras públicas, gestión financiera de los presupuestos asignados a TI, gestión documental, requerimientos de la Contraloría e incluso de otras áreas del MICITT. Es una realidad que hay un recargo de funciones excesiva, la administración lo conoce, pero... si las cosas no se hacen, hay sanciones. El techo presupuestario que impone MinHda debe tratarse a nivel gerencial, pues los Jerarcas priorizan lo que consideran sustantivo a la institución, no lo relativo a TI. Y los Jerarcas y la Administración siguen considerando que la ciberseguridad es materia y gestión únicamente de TI; no se involucran ni comprometen.
18	Generar conciencia y cultura en los Altos Jerarcas con el fin de que todos vayan en la misma línea. Minimizar la brecha de conocimiento a la población en general de lo que es ciberseguridad con un vocabulario no técnico. Pensando en un trabajo en Equipo interinstitucional inicialmente, tomando las más críticas del gobierno (prioridad) y posterior se van retomando las demás las cuales la idea es que se acoplen a una base ya establecida por el MICITT y este Equipo multidisciplinario.
19	Capacitación y recursos
20	Considerar la simplicidad en seguridad como una forma real y efectiva para las organizaciones, entre tanta complejidad la ciberseguridad pierde fuerza.
21	tenemos ides de incorporación de capacitación país
22	Importante determinar el método donde se nos solicite a los proveedores de las soluciones de Ciberseguridad, sea para recomendar las soluciones previo a las adquisiciones o compras, u ofertar RFP que ya estén creados entre Gobernanza Digital y la OEA, de manera que podamos, bajo una libre participación, aportar las soluciones respectivas, sin embargo, estableciendo las credenciales adecuadas de las empresas que estén en capacidad de proporcionar dichas soluciones, teniendo niveles adecuados con los fabricantes y estándares o normas, líderes y vigentes en la industria.
23	Entendemos que la estrategia de Ciberseguridad no ha tenido un hincapié especial en temas de RRHH. Ofrecemos nuestra participación y nos ponemos a la orden para que esta estrategia también incluya estos temas - tanto en planillas como en procesos propios de recursos humanos. Es necesario entender el mapeo y los riesgos, y si bien nuestra empresa no comercializa productos directos de ciberseguridad, si participamos en varios gobiernos en iniciativas similares y podemos compartir de las experiencias.

#	APORTES
24	Desarrollo de capacidades, habilidades y competencias para el Recurso Humano a cargo de todas estas actividades, iniciativas y proyectos, considerando además con las cantidades de personal adecuado para ello, empleando quizás mecanismos mixtos de aprovisionamiento de esto: Talento Propio y Talento de Terceros (tercerización).

Durante el mes de octubre de 2023, se subió al sitio web del MICITT el borrador de la Estrategia Nacional de Ciberseguridad de Costa Rica 2023-2027 a consideración de todas las múltiples partes interesadas bajo un proceso de consulta pública no vinculante hasta el día 25 de octubre de 2023, el cual puede ser visitado en el siguiente link.

Bajo dicho proceso de consulta, todas las múltiples partes interesadas (organizaciones del sector público, organizaciones del sector privado, organizaciones de sociedad civil, academia, entre otros) podrán presentar comentarios y recomendaciones al borrador por medio de la herramienta brindada.

Conclusiones

La estrategia cuenta con un Plan de Acción para reforzar la gobernanza de ciberseguridad, adecuar el marco normativo jurídico cibernético, mejorar la protección de infraestructuras y la ciber resiliencia nacional, fortalecer el ecosistema de ciberseguridad y cooperar activamente en el entorno digital. En dicho Plan de Acción se propone un listado de acciones estratégicas de corto, mediano y largo plazo basado en las mejoras prácticas internacionales y las actuales necesidades del país. La mayoría de las acciones serán implementadas por parte del MICITT no obstante algunas acciones requerirán del apoyo de varias entidades públicas.

ANEXO 1: Observaciones de la Consulta Pública No vinculante

Consulta al Marco Estratégico

Organización	Secciones generales	Propuesta de ajuste	Justificación de ajuste	Comentarios Adicionales		Estado	Consideración MICITT
José Alberto Gutierrez Salazar Director Legal y Regulatorio Liberty Telecomunicaciones de Costa Rica LY, S.A.	Marco Normativo	Exclusión Convenio Budapest	Se sugiere la exclusión de la normativa del Convenio de Budapest en la Estrategia Nacional de Ciberseguridad, con el fin de mantener una distinción clara entre el marco regulador del cibercrimen y el enfoque estratégico de la ciberseguridad en el ámbito de las TIC.	Ver oficio de respuesta		Revisada / No se acepta	El MICITT considera adecuado mencionar al Convenio de Europa sobre Ciberdelincuencia (Budapest, 2001) junto con su Segundo Protocolo Adicional como un instrumento internacional que tiene relación con la Estrategia Nacional de Ciberseguridad (ENC) en línea con la experiencia regional en la materia. Las siguientes ENC de la región mencionan al Convenio de Budapest en el marco normativo, en objetivos estratégicos y/o en líneas de acción relacionados con el combate a la ciberdelicuencia / cibercrímen: República Dominicana (2022), Ecuador (2022), Panamá (2021), Belize (2020), Costa Rica (2017), Colombia (2016).
	Enfoques Rectores	Incluir "Enfoque de Resiliencia"	En donde se reconoce la necesidad de articulación de los diferentes sectores y actores con las medidas necesarias para mantener la integridad, funcionamiento y capacidad de respuesta a pesar de los ataques cibernéticos, fallos de hardware o software u otras amenazas sobre la infraestructura crítica o servicios escenciales.			Se recibe comentario se analiza y el resultado del análisis no se requiere realizar cambios	El MICITT resalta que la ENC tiene como objeto general "Garantizar las condiciones para contar con un ecosistema nacional de ciberseguridad, seguro, resiliente e inclusivo que proteja de manera efectiva las infraestructuras críticas nacionales, los sectores público y privado y la ciudadanía de las ciber amenazas" y ha incluido como Pilar 3. Fortalecer la protección de infraestructuras y la ciber *resiliencia* nacional.

	Principios Orientadores	Incluir "Resiliencia"	Todos las partes interesadas deben asumir la responsabilidad de cooperar y contar con controles necesarios para asegurar la recuperación y articulación con los diversos sectores y actores para isolar cualquier riesgo cibernético que represente una amenza a la infraestrcutura crítica o servicios escenciales y la nación. Considerando aspectos de confidencialidad aplicables.			Se recibe comentario se analiza y el resultado del análisis no se requiere realizar cambios	El MICITT resalta que la ENC tiene como objeto general "Garantizar las condiciones para contar con un ecosistema nacional de ciberseguridad, seguro, resiliente e inclusivo que proteja de manera efectiva las infraestructuras críticas nacionales, los sectores público y privado y la ciudadanía de las ciber amenazas" y ha incluido como Pilar 3. Fortalecer la protección de infraestructuras y la ciber *resiliencia* nacional.
Jorge Torres Carrillo Director General Dirección de Inteligencia y Seguridad Nacional (DIS)		Agregar un apartado con la definición de ciber-soberania y resaltar la importancia de tomarlo en cuenta en esta Estrategia.	Entendiéndose como la necesidad de que nuestro país cuente con mecanismos que aseguren el control y respeto en el dominio del ciberespacio de las políticas nacionales y no traspaso de fronteras o limites como por ejemplo afectación a la soberanía costarricense, sobre todo en los efectos adversos que se puedan dar a las instituciones e infraestructura crítica por parte de actores externos.			Revisada / No se acepta	El MICITT no considera jurídicamente conveniente incluir en la ENC 2023-2027 una definición de cibersoberanía. No se hace mención alguna de este término a lo largo de la ENC.
		Agregar la definición de ciberterrorismo y la importancia de crear la capacidad de velar por este tema	Entendiéndose ciberterrorismo como la práctica de usar medios tecnológicos para causar terror e inestabilidad en un país o región para reivindicar posiciones políticas, estratégicas, religiosas, económicas o delictivas en detrimento del Estado Costarricense. Es importante desarrollar las capacidades de Inteligencia que permita conocer los alcances de actores maliciosos que pueden generar riesgo a nuestra nación			Revisada / No se acepta	El MICITT no considera jurídicamente conveniente incluir en la ENC 2023-2027 una definición de ciberterrorismo. No se hace mención alguna de este término a lo largo de la ENC.
		Promover la adquisición y utilización de herramientas de ciberinteligencia para anticipar y mitigar el riesgo de ser víctimas de futuros ciberataques.	Está comprobado que la mejor forma de prevención es la identificación de riesgos y vulnerabilidades ante actores que por lo general mantienen las mismas técnicas, tácticas y procedimientos para llevar acabo sus ataques contra las infraestructuras tecnológicas estatales exitosamente.			Revisada / No se acepta	El MICITT considera que la Línea de Acción 3.2 de la ENC 2023-2027 trata sobre el tema propuesto.
Daniel Rodríguez Maffioli Director | Digital Law & Policy ECIJA	Marco Normativo	Incluir dentro del Marco normativo la directriz No. 46 del 9 de abril de 2013 denominada "Las instituciones del sector público privilegiarán la adquisición de soluciones de cómputo en la nube sobre otro tipo de infraestructura".	Los servicios de infraestructrua, plataforma y software en la nube son demostradamente más seguros que los entornos "on-premise". Especialmente en Costa Rica,donde la inversión en seguridad de infraestructuras propias es escasa y las medidas de protección han demostrado ser muy frágiles (e.j. los ciberataques del 2022). Además, son servicios mucho más costo-eficientes, lo cual es una ventaja para países con recursos limitados como el nuestro.	La Estrategia de Ciberseguridad del país debe considerar la existencia de la directriz de nube, no solo por ser una Directriz vigente, sino por ser conveniente a los intereres de proteger los datos, redes e infraestructuras tecnológicas del país.		Se revisa y se traslada para análisis de DG	Se traslada la observación al Director de Gobernanza Digital para su valoración en el marco de las competencia de dicha Dirección

	Principios Orientadores	Creemos fundamental agregar un principio orientador consistente en "Apertura segura de datos y neutralidad tecnológica"	Es fundamental que Costa Rica mantenga su posición de apertura al mundo y al comercio digital internacional, sin restricciones localistas que restrinjan el flujo de datos con fundamento en nacionalismos tecnológicos que comprometerían la seguridad de la información, en lograr de mejorarla. La política del país en esta materia es de neutralidad tecnológica y libre acceso a servicios digitales transfronterizos, especialmente ahora con la aprobación del Tratado DEPA que está impulsando COMEX.			Revisada / No se acepta	El MICITT considera que los principios orientadores: i) Gestión integral de riesgos, ii) Respeto a los Derechos Humanos y los valores fundamentales, iii) Responsabilidad compartida, iv) Cooperación, y v) Innovación son adecuados para la ENC 2023-2027. En la experiencia regional no se encontró estrategia nacional de ciberseguridad alguna que haga referencia a lo propuesto.
Vera Bonilla Solís Gerente de Tecnología y Soluciones Digitales Instituto Costarricense de Electricidad (ICE)	Diagnóstico	Se recomienda cambiar la fuente de los datos en: *Gráfica 3. Evolución de las denuncias de delitos informáticos en Costa Rica.*	Tanto (SEMINARIO UNIVERSIDAD, 2023) & (LA NACION, 2023) son fuentes secundarias de esta información. Lo correcto es utilizar la fuente primaria de estos datos, en este caso, el Organismo de Investigación Judicial (OIJ) quien es la entidad oficial de Costa Rica en la recepción de este tipo de denuncias.	Una fuente secundaria describe, interpreta o sintetiza fuentes primarias. Datos provenientes de fuentes secundarias pueden contener filtraciones, interpretaciones o evaluaciones. Igualmente el nombre correcto del periódico es SEMANARIO UNIVERSIDAD, erroneamente se consigna como "SEMINARIO".		Revisada / Se acepta	El MICITT incluirá las cifras que presenten la evolución de las denuncias de delitos informáticos en Costa Rica que entregue el Organismo de Investigación Judicial (OIJ)
	Misión	Establecer un marco de acción integral que permita prevenir y mitigar los riesgos y amenazas en el entorno digital, fomentar la innovación y el desarrollo de soluciones en ciberseguridad, fortalecer la capacidad de respuesta ante incidentes de ciberseguridad, promover una cultura de seguridad sólida, con el fin de ayudar a garantizar la estabilidad del país y su economía, proteger la información personal y crítica del Estado y de la ciudadanía, y mantener la confianza en el uso de los sistemas digitales.	Mejora en la redacción: con el fin de ayudar.			Revisada / Se acepta	El MICITT acoge la propuesta de ajuste en la redacción.
	Objetivos Estratégicos	Garantizar que los procesos de gestión de riesgos de ciberseguridad y de gestión de riesgos de la seguridad de la información se integren en los procesos de planificación estratégica, operativa, y presupuestaria de las instituciones públicas.	Mejora en la redacción: gestión de riesgos.			Revisada / Se acepta	El MICITT acoge la propuesta de ajuste en la redacción.
Ana Lucía Ramírez Cámara INFOCOM	Contexto Actual de Ciberseguridad	Excluir las referencias a temas no relacionados con el fortalecimiento de la ciberseguridad, tal como son los factores geopolíticos.	Costa Rica es un país neutral, que no debería estar involucrado y mucho menos considerar asumir una posición hacia un bando u otro, en conflictos geopolíticos. Es importante no tomar la influencia de los factores geopoliticos como una determinante de esta Estrategia.	**Referencia**: Página 6. Párrafo 5. "Los eventos geopolíticos recientes también han influido significativamente en la estrategia cibernética"		Revisada / No se acepta	El MICITT resalta una situación ampliamente conocida a nivel internacional.

	Objetivos Estratégicos	Verificar con los operadores de servicios de telecomunicaciones y el ente regulador (SUTEL) sobre la forma correcta y viable de aplicar estos requerimientos	Esta propuesta es muy abierta y no considera los costos y recursos necesarios para la realización de auditorías de red; tal como se manifiesta en el Decreto de medidas de ciberseguridad para redes de telecomunicaciones 5G y superiores. Por otro lado, se hace un enfoque en la infraestructura de los operadores de servicios de telecomunicaciones, cuando en realidad los ataques no se han presentado debido a vulnerabilidades en estas redes; pero esta línea de acción da la impresión de que son el principal foco de problemas.	**Referencia**: Página 7. Líneas de Acción 3.3. "Proteger y defender las infraestructuras críticas nacionales y los operadores de servicios esenciales"		Revisada / No se acepta	Cabe señalar que las infraestructuras críticas no solo corresponden a Redes 5G sino que aborda plataformas tecnológicas donde residencien servicios esecianles para la ciudadanía y el país. Por lo tanto el abordaje se realiza de manera integral de múltiples acciones dentro de la estrategia.
	Principios Orientadores	Incluir la **neutralidad tecnológica** en los Principios orientadores	La neutralidad favorece la competencia y un entorno competitivo sano favorece la promoción de la innovación tecnológica.	**Referencia**: Página 16 . **4.5 Innovación** Los líderes y tomadores de decisiones que representan a las partes interesadas deben asegurarse de que la innovación sea considerada durante la implementación de iniciativas de ciberseguridad.		Revisada / No se acepta	El MICITT considera que los principios orientadores: i) Gestión integral de riesgos, ii) Respeto a los Derechos Humanos y los valores fundamentales, iii) Responsabilidad compartida, iv) Cooperación, y v) Innovación son adecuados para la ENC 2023-2027. En la experiencia regional no se encontró estrategia nacional de ciberseguridad alguna que haga referencia a lo propuesto. Además, este es un principio que se establece en ley General de Telecomunicaciones en el que se le otorga a los operadores y proveedores de servicios la potestad de seleccionar la tecnología por utilizada siempre que estas dispongan de estándares comunes y garantizados. Por lo anterior la observación se considera que aplique bajo un principio orientador de una Estrategia Nacional de Ciberseguridad.
	Principios Orientadores	**Agregar 4.6 Desarrollo**: Los líderes y tomadores de decisiones que representan a las partes interesadas deben equilibrar la seguridad con el desarrollo económico al desarrollar planes de ciberseguridad.	El objetivo final de ciberseguridad es promover la prosperidad y el desarrollo económico y social, e impulsar la transformación digital del país. La seguridad que obstaculiza el progreso social perderá su significado.	**Referencia**: Página 16 . 4.5 Innovación		Revisada / No se acepta	El MICITT considera que los principios orientadores: i) Gestión integral de riesgos, ii) Respeto a los Derechos Humanos y los valores fundamentales, iii) Responsabilidad compartida, iv) Cooperación, y v) Innovación son adecuados para la ENC 2023-2027. En la experiencia regional no se encontró estrategia nacional de ciberseguridad alguna que haga referencia a lo propuesto.

	Principios Orientadores	4.8.1. Reforzar la gobernanza de ciberseguridad Asegurar que la instancia de coordinación nacional cuente con un equipo de personal especializado, calificado y técnico dedicado a las acciones de ciberseguridad promoviendo la igualdad de género y la diversidad. y garantizar la independencia operativa de la organización.	Garantizar la independencia operativa de la organización.	**Referencia**: 4.8.1. Reforzar la gobernanza de ciberseguridad		Revisada / No se acepta	El MICITT no considera jurídicamente conveniente incluir en la ENC 2023-2027 el texto propuesto.
	Enfoques Rectores	Nombrar un director exclusivo para Ciber Gobernanza	Reestructuración del MICITT para reforzar su rol en materia de ciberseguridad			Revisada / No se acepta	El MICITT considera que la Línea de Acción 1.1 de la ENC 2023-2027 trata sobre el tema propuesto.
	Enfoques Rectores	Sugerir no solo la creación de la figura de enlace en ciberseguridad, sino del CISO o Chief information security officer a nivel central al menos, con amplias facultades de dirección.	Reestructuración del MICITT para reforzar su rol en materia de ciberseguridad. Este CISO debería estar habilitado para que su accionar sea “transversal” a lo largo de todas las instituciones públicas, generar política pública, y que coordine esfuerzos inclusive con sector privado.			Revisada / No se acepta	El MICITT considera que la Línea de Acción 1.2 de la ENC 2023-2027 trata sobre el tema propuesto.
	Participación social y ciudadana	Se reiteran los ofrecimientos de la Cámara INFOCOM para colaborar y cooperar en la materia de ciberseguridad; específicamente para temas de educación, prevención, y asesoría técnica.	Canalizar, por medio de la Cámara, los mecanismos específicos de cooperación con operadores de servicios esenciales, que incluyen los servicios de telecomunicaciones.			Revisada / No se acepta	El MICITT considera que la Línea de Acción 1.2 de la ENC 2023-2027 trata sobre el tema propuesto.
	Seguimiento, evaluación y gestión de riesgos	Instar a la Asamblea Legislativa y la Contraloría General de la República a que exijan que los presupuestos sometidos a su aprobación consideren los recursos financieros adecuados para la gestión integral de riesgos de ciberseguridad.	Gestión integral de riesgos de ciberseguridad.			Revisada / No se acepta	El MICITT ha resaltado el pronunciamiento de la Contraloría General de la República que hace referencia a lo mencionado (Ver Anexo 2 de la ENC 2023-2027)
	Alineación Estratégica	Proponer la regulación adecuada para la protección legal contra las amenazas cibernéticas y el resguardo y promoción de la innovación, en especial considerando los alcances del Plan de fomento a la creación de nuevas empresas	Reforzamiento de las capacidades del ecosistema de ciberseguridad.			Revisada / No se acepta	El MICITT no tiene facultadores para proponer dicha regulación. No obstante, la ENC 2023-207 establece en su Línea de Acción 2.1 que el MICITT apoyará a los reguladores sectoriales en el trámite de iniciativas o proyectos para adecuar, adaptar y/o armonizar el marco regulatorio relacionado con la ciberseguridad.
	Seguimiento, evaluación y gestión de riesgos	Valorar la oportunidad y la conveniencia de comunicar el contenido del Catálogo de infraestructuras críticas nacionales.				Revisada / No se acepta	El MICITT consdiera que la ENC 2023-2027 contiene las disposiciones y mecanimsos de comunicación adecuados para comunicar asuntos que se decidan bajo el modelo de gobernanza que se diseñe y ponga en marcha.
	Participación social y ciudadana	Evaluación en planes de respuesta inmediata y contingencia desde el Micitt para con la sociedad civil.	Con el objetivo de mitigar el impacto de posibles ciberataques en la cotidianidad de los habitantes de Costa Rica.			Revisada / No se acepta	El MICITT considera que la Línea de Acción 1.2 de la ENC 2023-2027 trata sobre el tema propuesto.

	Objetivos Estratégicos	Impulsar a través del SOC Nacional el establecimiento de una arquitectura única de elementos de detección y reacción inmediata en Ciberseguridad.	Fortalecer la detección y reacción inmediata en Ciberseguridad.			Revisada / No se acepta	El MICITT considera que la Línea de Acción 3.2 de la ENC 2023-2027 trata sobre el tema propuesto.
	Marco Normativo	Se solicita excluir la cita y referencia de la normativa del Convenio de Budapest, en esta Estrategia Nacional.	Mantener la claridad entre lo que es un marco regulatorio de cibercrimen y lo que es el enfoque estratégico de la ciberseguridad en materia de tecnologías de la información y comunicación TICs. El Convenio de Budapest no es considerado como un estándar internacional de ciberseguridad, pues su principal enfoque radica en el tratamiento, penalidades y persecusión internacional de los delitos cibernéticos.	**Referencia**: Apartado 2		Revisada / No se acepta	El MICITT considera adecuado mencionar al Convenio de Europa sobre Ciberdelincuencia (Budapest, 2001) junto con su Segundo Protocolo Adicional como un instrumento internacional que tiene relación con la Estrategia Nacional de Ciberseguridad (ENC) en línea con la experiencia regional en la materia. Las siguientes ENC de la región mencionan al Convenio de Budapest en el marco normativo, en objetivos estratégicos y/o en líneas de acción relacionados con el combate a la ciberdelicuencia / cibercrímen: República Dominicana (2022), Ecuador (2022), Panamá (2021), Belize (2020), Costa Rica (2017), Colombia (2016).
	Enfoques Rectores	Incluir "Enfoque de Resiliencia"	Se sugiere reconocer la necesidad de articulación de los difetentes sectores y actores con las medidas necesarias para mantener la integridad, funcionamiento y capacidad de respuesta, a pesar de los ataques cibernéticos, fallos de hardware o software u otras amenazas sobre la infraestrucuta crítica o servicios escenciales.			Revisada / No se acepta	El MICITT resalta que la ENC tiene como objeto general "Garantizar las condiciones para contar con un ecosistema nacional de ciberseguridad, seguro, resiliente e inclusivo que proteja de manera efectiva las infraestructuras críticas nacionales, los sectores público y privado y la ciudadanía de las ciber amenazas" y ha incluido como Pilar 3. Fortalecer la protección de infraestructuras y la ciber *resiliencia* nacional.
	Principios Orientadores	Incluir "Resiliencia"	Todos las partes interesadas deben asumir responsabilidad de cooperar y contar con controles necesarios para asegurar la recuperación y articulación con los diversos sectores y actores para isolar cualquier riesgo cibernético que represente una amenza a la infraestrcutura crítica o servicios escenciales y la nación. Considerando aspectos de confidencialidad aplicables.			Revisada / No se acepta	El MICITT resalta que la ENC tiene como objeto general "Garantizar las condiciones para contar con un ecosistema nacional de ciberseguridad, seguro, resiliente e inclusivo que proteja de manera efectiva las infraestructuras críticas nacionales, los sectores público y privado y la ciudadanía de las ciber amenazas" y ha incluido como Pilar 3. Fortalecer la protección de infraestructuras y la ciber *resiliencia* nacional.

Federico Chacón Loaiza Presidente Consejo de la SUTEL	Principios Orientadores	Los principios de “competencia efectiva”, de “no discriminación” y de “neutralidad tecnológica” contenidos en la Ley General de Telecomunicaciones, Ley 8642, deberían incorporarse a la sección “4.5 Principios orientadores” de la propuesta, en virtud de que su adopción mantendría invariable el objetivo perseguido, pero encausaría su consecución a través de mecanismos que impliquen condiciones de igualdad y posibilidades de diferenciación en materia de servicios de telecomunicaciones.				Revisada / No se acepta	El MICITT considera que los principios orientadores: i) Gestión integral de riesgos, ii) Respeto a los Derechos Humanos y los valores fundamentales, iii) Responsabilidad compartida, iv) Cooperación, y v) Innovación son adecuados para la ENC 2023-2027. En la experiencia regional no se encontró estrategia nacional de ciberseguridad alguna que haga referencia a lo propuesto. Además, este es un principio que se establece en ley General de Telecomunicaciones en el que se le otorga a los operadores y proveedores de servicios la potestad de seleccionar la tecnología por utilizada siempre que estas dispongan de estándares comunes y garantizados. Por lo anterior la observación se considera que aplique bajo un principio orientador de una Estrategia Nacional de Ciberseguridad.
	Principios Orientadores	Es esencial respetar el principio de neutralidad. Entidades que se dediquen a actividades similares deben estar sujetas a reglas igualmente similares preservando su capacidad de elegir, adoptar y emplear tecnologías, infraestructuras y modelos de negocio de su elección para competir. Además, cuando ciertas empresas controlan los recursos necesarios para llevar a cabo una actividad, es fundamental garantizar un acceso equitativo y no discriminatorio a estos recursos, permitiendo así que los nuevos competidores puedan competir con los ya establecidos.				Revisada / No se acepta	El MICITT considera que los principios orientadores: i) Gestión integral de riesgos, ii) Respeto a los Derechos Humanos y los valores fundamentales, iii) Responsabilidad compartida, iv) Cooperación, y v) Innovación son adecuados para la ENC 2023-2027. En la experiencia regional no se encontró estrategia nacional de ciberseguridad alguna que haga referencia a lo propuesto.

		Es fundamental que, se consideren tanto los impactos positivos como los negativos que la propuesta pueda tener en la sociedad y en la economía en general, mediante un análisis que pondere el costo de su implementación para todos aquellos sujetos bajo su alcance en contraposición con los beneficios que se proyectan. La propuesta fundamenta su validez si los beneficios que produciría superan los costos asociados, a su cumplimiento. En muchas ocasiones, las cargas regulatorias imponen cargas administrativas a las empresas, especialmente a las nuevas o a las pequeñas, lo que puede reducir la capacidad que estas empresas pueden orientar a la innovación. La presencia de regulaciones duplicadas y poco eficientes también puede perjudicar la economía en general. Las propuestas deben plantearse en la medida de lo posible pensando en la menor perturbación sobre la competencia. Para esto es crucial que se realice una evaluación exhaustiva de las posibles alternativas por medio de un análisis que considere tanto su eficacia para abordar la problemática que se pretende atender como el grado de interferencia que podría generar en el funcionamiento de los mercados.				Revisada / No se acepta	Se hace mención que esta es una Estrategia Nacional De ciberseguridad tiene como fin mejorar la ciberseguridad en todos los sectores. Razón por la cual se realizó la construcción de la misma con la participación de todos los interesados (sector público, privado, sociedad y academia). Además, los aspectos de compentencia excenden el alcance de las acciones establecidas de ésta Estrategia.
		Cualquier potencial imposición que devenga sustentada en esta estrategia debería siempre procurar no incidir en los estímulos propios de los mercados abiertos para que se dé una competencia vigorosa. Debe permitirse entonces que las empresas tengan la oportunidad de destacarse unas de otras al ofrecer características distintivas que atraigan a los consumidores, particularmente en aspectos específicos que influyan en el resultado de la competencia en cada mercado.				Revisada / No se acepta	Las acciones de la presente estrategia no aborda o impone condiciones para el mercado o adquisición de tecnología. Dicha estrategia está enfocada en abordar la ciberseguridad de manera integral pensando en madurar la postura de ciberseguridad del ecosistema nacional mediante acciones que fortalezcan las infraestructuras sin obstaculizar los mercados.

Pilar 1. Gobernanza y Coordinación

Organización	Línea de Acción	Propuesta de ajuste	Justificación de ajuste	Comentarios Adicionales		Estado	Consideración MICITT
José Alberto Gutierrez Salazar Director Legal y Regulatorio Liberty Telecomunicaciones de Costa Rica LY, S.A.	Línea de Acción 1.1	Socializar el modelo de coordinación nacional	Es necesario que todas las instancias y actores de la academia, industra y terceras partes conozcan el modelo propuesto y sepan cuales son sus actividades, roles y responsabilidades			Revisada / No se acepta	El MICITT considera que la Línea de Acción 1.1 de la ENC 2023-2027 trata sobre el tema propuesto. Para definir el marco de gobernanza es necesario definir roles y responsabilidades de las partes interesadas en el ecosistema de ciberseguridad.
	Línea de Acción 1.2	Definir con claridad los roles y responsabilidades de todos los participantes de la industria, acedemia y gobierno en el modelo de gobernanza	Para que un modelo de gobernanza exista es necesario que todos los roles existan			Revisada / No se acepta	El MICITT considera que la Línea de Acción 1.2 de la ENC 2023-2027 trata sobre el tema propuesto. Para definir el marco de gobernanza es necesario definir roles y responsabilidades de las partes interesadas en el ecosistema de ciberseguridad.

Jorge Torres Carrillo Director General Dirección de Inteligencia y Seguridad Nacional (DIS)	Línea de Acción 1.1	Es necesario incluir a la Dirección de Inteligencia y Seguridad Nacional (DIS) dentro del comité consultivo.	Según la Ley 7410, articulo 13°, se crea la DIS como un órgano informativo del Presidente en materia de Seguridad Nacional, de esta manera es de suma importancia la integración de nuestra institución a la Estrategia Nacional de Ciberseguridad como un pilar importante en la Coordinación Nacional y la información que debe de tener de primera mano el Presidente ante escenarios de crisis generados por incidentes cibernéticos, aparte de esto la DIS posee la capacidad de realizar una coordinación eficiente con servicios homólogos internacionales lo cual quedó evidenciado en la atención de los incidentes cibernéticos del 2022. Según artículo 14° de la misma Ley, dentro de las atribuciones de la DIS esta detectar, investigar, analizar y comunicar al Presidente de la República o al Ministro de la Presidencia, la información necesaria para prevenir hechos que impliquen riesgo para la independencia o la integridad territorial o pongan en peligro la estabilidad del país y de sus instituciones. Desde esta óptica la integración de la DIS a este comité se observa como más que necesaria, ya que la institución tiene la capacidad de realizar análisis en prospectiva de fenómenos que impliquen riesgos para el país			Revisada / Se acepta	El MICITT ha mencionado explícitamente a la Dirección de Inteligencia y Seguridad Nacional (DIS) como entidad de apoyo para la creación del marco de gobernanza nacional de ciberseguridad.
Daniel Rodríguez Maffioli Director | Digital Law & Policy ECIJA	Línea de Acción 1.1	Aclarar qué es la "instancia de coordinación nacional de ciberseguridad". Si se trata de un nuevo órgano a lo interno del MICITT, una Agencia, la Dirección de Ciberseguridad.	No queda claro qué es la "instancia de coordinación de ciberseguridad", o si es la instancia que se definirá vía ley o vía Plan de restructuración.			Revisada / No se acepta	El MICITT considera que la Línea de Acción 1.1 de la ENC 2023-2027 trata sobre el tema propuesto.

	Línea de Acción 1.3	Agregar una línea de acción consistente en Crear un plan (a más tardar el 2024) de migración y modernización de TI del Estado, que privilegia los servicios seguros en la nube, con el objetivo de dotar de mayor seguridad a los sistemas y datos del Estado costarricense.	La meta debería ser que en 2027 el 80% del Estado tenga una infraestructura moderna, segurra y en la nube. La experiencia de Hacienda Digital puede servir de ejemplo y guía. Pero es trascendental esa migración para garantizar que la información de los costarricenses está protegida. Además, esta modernización ayudaría a mejorar la prestación de servicios digitales según la Estrategia de Transformación Digital.	Se sugiere incluir metas de plazos para ir logrando esta migración.		Revisada / No se acepta	Se traslada la observación al Director de Gobernanza Digital para su valoración en el marco de las competencia de dicha Dirección
Vera Bonilla Solís Gerente de Tecnología y Soluciones Digitales Instituto Costarricense de Electricidad (ICE)	Línea de Acción 1.2	Cuadro de Responsabilidad. Puntos 5,6,7. Incluir MSP como responsable y como apoyo al OIJ	Por sus roles y responsabilidad			Revisada / Se acepta	El MICITT considera adecuado contar con el apoyo de las entidades mencionadas
	Línea de Acción 1.3	En el punto 2 "Desarrollar un plan de inversión que garantice la disponibilidad y asignación de recursos suficientes en instituciones públicas para llevar a cabo iniciativas de ciberseguridad".	Consideramos que debe eliminarse en vista de que el punto 4 lo incluye en acuerdo a la línea administrativa de cada insitución. O aclarar la redacción.			Revisada / No se acepta	El MICITT considera que la Línea de Acción 1.3 de la ENC 2023-2027 trata sobre el tema propuesto.

	Línea de Acción 1.3	Se propone incluir un punto adicional que considere lo siguiente: "Desarrollar y ejecutar un plan financiero que garantice la disponibilidad y asignación de recursos suficientes en las instituciones públicas para enfrentar la atención de emergencias ante incidentes de seguridad cibernética" o de lo contrario, instruir para que cada institucion o empresas del sector publico hagan la presupuestacion anual.	Obedece a la previsión de recursos financieros para la atención de emergencias cibernéticas. Se recomienda eliminar la palabra promover, ya que con ella queda a la libre la obligacion de invertir en ciberseguridad.			Revisada / No se acepta	El MICITT considera que la Línea de Acción 1.3 de la ENC 2023-2027 trata sobre el tema propuesto.

Pilar 2. Marco Legal y Regulatorio

Organización	Línea de Acción	Propuesta de ajuste	Justificación de ajuste	Comentarios Adicionales		Estado	Consideración MICITT
José Alberto Gutierrez Salazar Director Legal y Regulatorio Liberty Telecomunicaciones de Costa Rica LY, S.A.	Línea de Acción 2.1	Agregar el ecosistema digital en relación con el marco jurídico cibernético	Que todos las partes interesadas conozcan sus responsabilidades en medio del marco jurídico contribuira a poder definir claramente los marcos de acción facilitando la integración de acciones en medio de ataques cibernéticos			Revisada / No se acepta	El MICITT considera que la Línea de Acción 1.2 de la ENC 2023-2027 trata sobre el tema propuesto. Para definir el marco de gobernanza es necesario definir roles y responsabilidades de las partes interesadas en el ecosistema de ciberseguridad.
	Línea de Acción 2.2	Construir modelos de interoperación para la gestión de riesgo cibernético	Algunas organizaciones que soportan infraestructura crítica ya cuentan con modelos de gestión de riesgo cibernéticos, es por ello que se hace necesario que se piense en criterios de interoperatibilidad entre los modelos creados por la nación y los operadores de infraetsructura crítica			Revisada / No se acepta	El MICITT considera que la Línea de Acción 3.1 (Adoptar un marco para la gestión integral de riesgos de ciberseguridad) de la ENC 2023-2027 trata sobre el tema propuesto.
Vera Bonilla Solís Gerente de Tecnología y Soluciones Digitales Instituto Costarricense de Electricidad (ICE)	Línea de Acción 2.1	Cuadro de Responsabilidad. Puntos 18,20. Incluir MP, MSP como responsable y como apoyo al OIJ, Universidades Públicas, PGR, Defensoría de los Habitantes.	Por sus roles y responsabilidad			Revisada / No se acepta	El MICITT considera que la Línea de Acción 2.1 de la ENC 2023-2027 trata sobre el tema propuesto.

	Línea de Acción 2.1	Se recomienta hacer una actualizacion integral del marco legal y regulatorio cibernético haciendo énfasis en el entorno internacional de acuerdo al uso publico de apps y sistemas para la protección legal contra las amenazas cibernéticas basadas en género con perspectiva interseccional, previniendo, sancionando y erradicando la violencia de género facilitada por las tecnologías digitales.	Muchos de los aplicativos utilizados por la población y con dominio en el extranjero aplican en sus políticas las leyes de su país y dan la facilidad de aplicar las políticas en el país de uso pero nuestra legislación al no tener estos elementos no es posible adaptar estos aplicativos a nuestra legislación			Revisada / No se acepta	El MICITT considera que la Línea de Acción 2.1 de la ENC 2023-2027 trata sobre el tema propuesto.
	Línea de Acción 2.2	En el punto 3, "Desarrollar un marco normativo para la protección de infraestructuras críticas nacionales y de operadores de servicios esenciales…". **Se propone reemplazar por:** Revisar iniciativas, proyectos y desarrollar un marco normativo para la protección de infraestructuras criticas....	Debido a que existen iniciativas legislativas en esa materia.			Revisada / No se acepta	El MICITT considera que la Línea de Acción 2.1 de la ENC 2023-2027 menciona el apoyo tanto a la Asamblea Legislativa en el trámite de iniciativas o proyectos para adecuar, adaptar y/o armonizar el marco legal relacionado con la ciberseguridad.

Federico Chacón Loaiza Presidente Consejo de la SUTEL		Garantizar la seguridad jurídica a través de un marco jurídico claro, específico y enfocado en su objetivo principal. Debe evitarse cualquier tipo de ambigüedad que pueda afectar a quienes se encuentran bajo su alcance; esto pues no debe olvidarse que, las empresas, especialmente las emergentes, pueden proporcionalmente enfrentar costos de cumplimiento más altos, y la regulación podría convertirse en una barrera para su entrada al mercado				Revisada / Se acepta	El MICITT considera que la Línea de Acción 2.1 de la ENC 2023-2027 trata sobre el tema propuesto.

Pilar 3. Protección de Infraestructuras y ciber resiliencia

Organización	Línea de Acción	Propuesta de ajuste	Justificación de ajuste	Comentarios Adicionales		Estado	Consideración MICITT
José Alberto Gutierrez Salazar Director Legal y Regulatorio Liberty Telecomunicaciones de Costa Rica LY, S.A.	Línea de Acción 3.1	Se hace necesario construir modelos de interoperación para la gestión de riesgo cibernético	Algunas organizaciones que soportan infraestructura crítica ya cuentan con modelos de gestión de riesgo cibernéticos, es por ello que se hace necesario que se piense en criterios de interoperatibilidad entre los modelos creados por la nación y los operadores de infraetsructura crítica			Revisada / No se acepta	El MICITT considera que la Línea de Acción 3.1 (Adoptar un marco para la gestión integral de riesgos de ciberseguridad) de la ENC 2023-2027 trata sobre el tema propuesto.
	Línea de Acción 3.2	Crear y ejecutar una estrategia para promover la creación y el fortalecimiento de SOC sectoriales. **Eliminar**	La cooperación intersectorial deberá siempre ser articulada ante el ente de gobierno designado SOC o CSIRT, no se recomienda por los sectores propiamente.			Revisada / No se acepta	El MICITT considera adecuada esta acción en línea con la experiencia regional.
	Línea de Acción 3.2	Proyectar la integración de las capacidades del SOC-CR con las empresas del sector privado que cuentan con estás capacidades	Es importante que existan mecanismos de integración para expandir las capacidades de monitoreo del SOC-CR y que existan lineamientos claros para estas integraciones			Revisada / No se acepta	El MICITT considera que la Línea de Acción 3.2 de la ENC 2023-2027 trata sobre el tema propuesto.
	Línea de Acción 3.3	Adelantar evaluaciones de riesgos de ciberseguridad de las infraestructuras críticas nacionales en conjunto con los operadores de servicios esenciales. mover a 2024: 3		Se debe tipificar el marco de trabajo para las evaluaciones de gestión de riesgo.		Revisada / No se acepta	El MICITT considera que la Línea de Acción 3.3 de la ENC 2023-2027 trata sobre el tema propuesto.

	Línea de Acción 3.3	Establecer el modelo de responsabilidades	Si bien existen operdores de infraestructuras críticas, es bueno que las relaciones, roles y responsabilidades queden bien definidos. En especial en relación con la gestión de riesgo cibernético, la definición y ejecución de los planes de acción	La coordinación de este tipo de ejercicio se sugiere se haga al menos con un mes de antelación.		Revisada / No se acepta	El MICITT considera que la Línea de Acción 1.2 de la ENC 2023-2027 trata sobre el tema propuesto. Para definir el marco de gobernanza es necesario definir roles y responsabilidades de las partes interesadas en el ecosistema de ciberseguridad, incluidos a todos los operadores que ejercen el control sobre las infraestructuras críticas nacionales y prestan servicios esenciales
	Línea de Acción 3.4	Definición de parámetros de reporte de incidentes	Basados en las situaciones actuales como el modelo de la SEC (Security Exchange Commission) y otros, que ya han definido los criterios para el reporte de incidentes, es bueno que se dejen claras de acuerdo a las capacidades actuales todos estos criterios que ayuden a fortalecer el ecosistema de la nación			Revisada / No se acepta	El MICITT considera que la Línea de Acción 3.4 de la ENC 2023-2027 trata sobre el tema propuesto.
	Línea de Acción 3.4	Crear y poner en marcha un mecanismo de notificación a personas u organizaciones afectadas por incidentes de ciberseguridad				Revisada / No se acepta	El MICITT considera que la Línea de Acción 3.4 de la ENC 2023-2027 trata sobre el tema propuesto.
Daniel Rodríguez Maffioli Director | Digital Law & Policy ECIJA	Línea de Acción 3.2	Se sugiere incorporar breve mención del principios de libre competencia en la selección de proveedores del SOC y de proveedores cloud que soportarán al SOC	La creación de un SOC debe ir precedida de un concurso que garantice que el Estado recibirá la mejor solución posible y acorde a sus necesidades. Esto solo se garantiza permitiendo una amplia participación de empresas en un concurso transparente y libre.			Revisada / No se acepta	El MICITT considera que la Línea de Acción 3.2 de la ENC 2023-2027 trata sobre el tema propuesto.

	Línea de Acción 3.2	Se recomienda indicar un porcentaje de avance en la intervención pública 31 (SOC permanente) para los años 2024 y 2025, p.e. avanzar un 10% en 2024 y un 15% en 2025.	De esta manera se puede ir avanzando y midiendo ese progreso en los próximos dos años.			Revisada / Se acepta	El MICITT considera adecuado ajustar el avance de cumplimiento de la meta para el indicador mencionado.
	Línea de Acción 3.2	Aclarar la diferencia entre SOCs pues no queda claro, y mencionar criterios generales bajo los cuales se priorizarán las instituciones "conectada" al SOC inicial.				Revisada / No se acepta	El MICITT considera que la Línea de Acción 3.2 de la ENC 2023-2027 trata sobre el tema propuesto.
	Línea de Acción 3.2	En la intervención pública 33, incluir como Co-Responsables a algunos reguladores de sectores críticos, por ejemplo, CONASSIF, Ministerio de Salud, CETAC, ARESEP y SUTEL.	Los reguladores sectoriales deberían participar en la elaboración de la Estrategia de SOCs sectoriales pues les afectarán y podrían tener que poner recursos propios para ello			Revisada / No se acepta	El MICITT considera que los reguladores sectoriales son entidades de apoyo para implementar la acción mencionada.
Vera Bonilla Solís Gerente de Tecnología y Soluciones Digitales Instituto Costarricense de Electricidad (ICE)	Línea de Acción 3.3	Identificar, categorizar y actualizar las infraestructuras críticas nacionales y los operadores de servicios esenciales	Es necesario que la acción de actualización quede establecida en el objetivo tal y como fue definido el indicador			Revisada / No se acepta	El MICITT considera que la Línea de Acción 3.3 de la ENC 2023-2027 trata sobre el tema propuesto.
	Línea de Acción 3.4	Revisar término "compartición"				Revisada / No se acepta	El MICITT considera adecuado el uso del término.
	Línea de Acción 3.4	Cuadro de Responsabilidad. Puntos 39. Incluir como apoyo al OIJ	Por sus roles y responsabilidad			Revisada / No se acepta	El MICITT considera que el OIJ como entidad de apoyo para implementar la acción mencionada.

	Línea de Acción 3.4	Los acceso a los mecanismos de notificación de incidentes de ciberseguridad deben ser restringidos y actualizados mensualmente. Indicados en los objetivos 41 y 42	Establecer una gestión controlada al acceso de la información de los incidentes de ciberseguridad nacional, y ser únicamente comunicados mediante el canal oficial.			Revisada / No se acepta	El MICITT considera que la Línea de Acción 3.4 de la ENC 2023-2027 trata sobre el tema propuesto.
Edith Guevara Espinoza Gerencia de Tecnología y Soluciones Digitales Dirección Ciberseguridad-Seguridad de la Información Instituto Costarricense de Electricidad (ICE)	Línea de Acción 3.4	Creo que los riesgos que más afectan a la sociedad están el robo de información, de dinero de cuentas bancarias, phishing, de suplantación de identidad, de explotación sexual, entre otros. Mencionan mucho el tema de género, sin embargo, creo que hay otros riesgos mayores				Revisada / No se acepta	El MICITT considera que la Línea de Acción 3.4 de la ENC 2023-2027 trata sobre el tema propuesto.

Pilar 4. Educación, Capacitación y Concientización

Organización	Línea de Acción	Propuesta de ajuste	Justificación de ajuste	Comentarios Adicionales		Estado	Consideración MICITT
Daniel Rodríguez Maffioli Director | Digital Law & Policy ECIJA	Línea de Acción 4.3	Incluir mención expresa a privilegiar desarrollos que incorporen inteligencia artificial para mejorar la posición de cberseguridad de gobierno y empresas.	La IA está mejorando significativamente la capacidad de detección de ataques y de prevención. Sería importante desarrollar soluciones propias en el país con apoyo de unviersidades, o valorar también soluciones de código abierto o de bajo costo en el mercado, para implementar en el sector público.	En los recursos requeridos para esta línea de acción, se sugiere incorporar fondos de investigación y desarrollo que maneja la Promotora de Investigación, y las universidade estatales. Además, incluirlas como Co-responsables.		Revisada / No se acepta	El MICITT considera que la Línea de Acción 4.3 de la ENC 2023-2027 trata sobre el tema propuesto.
Vera Bonilla Solís Gerente de Tecnología y Soluciones Digitales Instituto Costarricense de Electricidad (ICE)	Línea de Acción 4.1	Cuadro de Responsabilidad. Puntos 44, 45, 46, 47, 50. Incluir como apoyo a Universidades Públicas, INA	Por sus roles y responsabilidad			Revisada / Se acepta	El MICITT considera adecuado contar con el apoyo de las entidades mencionadas
	Línea de Acción 4.1	Recursos requeridos para los objetivos 44 al 50; incluir alianza publico - privada	Se debe valorar el incluir en esta columna la alianza publico - privada ya que facilitara el llegar a mas población principalmente estudiantil y es de interés de las empresas darse a conocer.			Revisada / No se acepta	El MICITT considera que la Línea de Acción 5.1 de la ENC 2023-2027 trata sobre el tema propuesto.
	Línea de Acción 4.1	Cuadro de Responsabilidad. Punto 49. Incluir como apoyo al OIJ, MP, MSP, Corte Suprema de Justicia, PGR	Por sus roles y responsabilidad			Revisada / Se acepta	El MICITT considera que las entidades mencionadas ya están incluidas, a excepción de la PGR.

	Línea de Acción 4.2	Cuadro de Responsabilidad. Puntos 51, 53. Incluir como apoyo a Universidades Públicas, INA	Por sus roles y responsabilidad			Revisada / Se acepta	El MICITT considera adecuado contar con el apoyo de las entidades mencionadas
	Línea de Acción 4.3	Cuadro de Responsabilidad. Puntos 55, 56, 58. Incluir como apoyo a Universidades Públicas, INA	Por sus roles y responsabilidad			Revisada / Se acepta	El MICITT considera adecuado contar con el apoyo de las entidades mencionadas
Edith Guevara Espinoza Gerencia de Tecnología y Soluciones Digitales Dirección Ciberseguridad-Seguridad de la Información Instituto Costarricense de Electricidad (ICE)	Línea de Acción 4.1	Se debería mencionar con prioridad incluso mayor a estas, la explotación sexual a niños, niñas y adolescentes, que están dentro de las estrategias que promueve el MICITT (EASNNAL)				Revisada / No se acepta	El MICITT considera que la Línea de Acción 4.2 de la ENC 2023-2027 trata sobre el tema propuesto.
	Línea de Acción 4.2	Más que solo el enfoque de género, pienso que podría enmarcarlo en "iguadad de género"				Revisada / No se acepta	El MICITT considera que la Línea de Acción 4.2 de la ENC 2023-2027 trata sobre el tema propuesto.
	Línea de Acción 4.2	No menciona la EASNNAL				Revisada / No se acepta	El MICITT incluye a la EASNNAL en el numeral 4.1 (Alienación Estratégica) de la ENC 2023-2027

Pilar 5. Cooperación y Alianzas

Organización	Línea de Acción	Propuesta de ajuste	Justificación de ajuste	Comentarios Adicionales	Estado	Consideración MICITT
Daniel Rodríguez Maffioli Director | Digital Law & Policy ECIJA	Línea de Acción 5.1	Valorar incluir una intervención en este eje consistente en desarrollar un Decreto de alianzas público-privadas tecnológicas.	El decreto de asociaciones público-privadas existente aplica principalmente a obras públicas, y no a proyectos tecnológicos. Esto permitiría a las entidades entender cómo proceder con estas alianzas y fomentaría su realización en un marco de seguridad jurídica. La empresa privada es una aliada fundamental de la ciberseguridad.	Definir plazo para su realización y Responsable	Revisada / No se acepta	El MICITT no considera jurídicamente conveniente incluir en la ENC 2023-2027 el texto propuesto.

MINISTERIO DE CIENCIA, INNOVACIÓN, TECNOLOGÍA Y TELECOMUNICACIONES

GOBIERNO DE COSTA RICA

GEZER RAMIRO MOLINA COLOMER (FIRMA)
PERSONA FISICA, CPF-01-1239-0030.
Fecha declarada: 12/11/2023 10:53:46 PM
Esta es una representación gráfica únicamente, verifique la validez de la firma.

Gezer Ramiro Molina Colomer

Director de Ciberseguridad

Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones